



Dr.WEB

for UNIX Internet Gateways

管理者マニュアル



© Doctor Web, 2024無断複写・転載を禁じます。

本マニュアルは特定のDr.Webソフトウェアの使用に関する情報を提供し、参照目的で用いられることを意図したものです。Dr.Webソフトウェアに特定の機能や技術仕様が備わっているかどうかを包括的に示すものではなく、また、Dr.Webソフトウェアが特定の要件や技術的仕様／パラメータ、他社製品のマニュアルに適合するかどうかを判断するために使用するものではありません。

本マニュアルの著作権はDoctor Webが有し、製品購入者が個人的目的でのみ使用することができます。本マニュアルのいなる部分も、購入者の私的利用以外の目的で、いかなる形式または方法によっても無断で複製、出版、送信することを禁じます。

商標

Dr.Web、SpIDer Mail、SpIDer Guard、CureIt!、CureNet!、AV-Desk、KATANA、Dr.WEBロゴは、ロシアおよびその他の国におけるDoctor Webの商標および登録商標です。本マニュアルに記載されているその他の商標、登録商標、および会社名の著作権はそれぞれの所有者が有します。

免責事項

Doctor Webおよびそのリセラー、ディストリビューターは、本マニュアル内の誤りや記載漏れについて責任を負わず、本マニュアルの使用や本マニュアルに含まれる情報を使用できないことによって（直接的、間接的を問わず）引き起こされた、または引き起こされたと主張されるいかなる損害に対しても責任を負わないものとします。

Dr.Web for UNIX Internet Gateways

バージョン**11.1**

管理者マニュアル

2024/02/01

Doctor Webロシア本社

2-12A, 3rd str. Yamskogo polya, Moscow, Russia, 125124

ウェブサイト: <https://www.drweb.com/>

電話番号: +7 (495) 789-45-87

支社および海外オフィスについては、Doctor Web公式サイトをご覧ください。

Doctor Web

Doctor Webは、悪意のあるソフトウェアやスパムからの効果的な保護を提供するDr.Web情報セキュリティソリューションの開発および販売を行っています。

世界中の個人ユーザーから政府機関、中小企業、大企業まで幅広いカスタマーに支持されています。

Dr.Webアンチウイルスソリューションは、マルウェア検出と国際情報セキュリティ基準への準拠における持続的な卓越性によって1992年よりその名を広く知られています。

Dr.Webソリューションに与えられた数々の認定や賞、そして世界中に広がるユーザーが、製品の持つ並外れた信頼性を示す何よりの証です。

Dr.Web製品をご利用いただき誠にありがとうございます。



目次

はじめに	8
表記規則と略語	9
この製品について	10
Dr.Web for UNIX Internet Gateways のメイン機能	10
Dr.Web for UNIX Internet Gateways の構成	12
隔離への移動	19
ファイルのパーミッションと権限	20
動作モード	21
システム要件と互換性	24
ライセンス	28
インストールとアンインストール	29
Dr.Web for UNIX Internet Gateways をインストールする	30
ユニバーサルパッケージをインストールする	31
コマンドラインからインストールする	32
リポジトリからインストールする	33
Dr.Web for UNIX Internet Gateways をアップグレードする	36
パッケージとコンポーネントを更新する	36
新しい製品バージョンにアップグレードする	37
インターネットに接続せずにデータベースを更新する	40
Dr.Web for UNIX Internet Gateways をアンインストールする	41
ユニバーサルパッケージをアンインストールする	41
コマンドラインからアンインストールする	42
リポジトリからインストールした Dr.Web for UNIX Internet Gateways をアンインストールする	42
追加情報	45
Dr.Web for UNIX Internet Gateways パッケージとファイル	45
コンポーネントのカスタムインストールとアンインストール	48
セキュリティサブシステムを設定する	53
SELinuxのセキュリティポリシーを設定する	53
開始する	57
製品の登録と有効化	57
製品の動作確認	60
Squid プロキシサーバーとの統合	61
ローカル Web サーバーを保護する	65



SpIDer Gateをプロキシモードで使用する	67
簡単な説明	70
Dr.Web for UNIX Internet Gatewaysコンポーネント	75
Dr.Web ConfigD	75
動作原理	75
コマンドライン引数	76
設定パラメータ	77
Dr.Web Ctl	81
コマンドライン呼び出しフォーマット	83
使用例	110
設定パラメータ	114
Dr.Web 管理Webインターフェース	115
コンポーネントを管理する	116
脅威の管理	117
設定を管理する	119
集中管理モードの管理	123
ローカルファイルをスキャンする	124
Dr.Web ICAPD	128
動作原理	128
コマンドライン引数	131
設定パラメータ	131
LuaでのHTTPメッセージ処理	146
SpIDer Gate	163
動作原理	164
コマンドライン引数	165
設定パラメータ	165
Dr.Web Firewall for Linux	168
動作原理	168
コマンドライン引数	173
設定パラメータ	173
Luaでの接続処理	198
Dr.Web ClamD	206
動作原理	206
コマンドライン引数	206
設定パラメータ	207
外部アプリケーションとの統合	213



Dr.Web File Checker	215
動作原理	215
コマンドライン引数	216
設定パラメータ	216
Dr.Web Network Checker	219
動作原理	219
コマンドライン引数	221
設定パラメータ	222
スキャンクラスタの作成	226
Dr.Web Scanning Engine	230
動作原理	230
コマンドライン引数	231
設定パラメータ	234
Dr.Web Updater	236
動作原理	236
コマンドライン引数	237
設定パラメータ	238
Dr.Web ES Agent	244
動作原理	244
コマンドライン引数	244
設定パラメータ	245
Dr.Web HTTPD	248
動作原理	248
コマンドライン引数	249
設定パラメータ	249
HTTP APIの説明	252
Dr.Web SNMPD	274
動作原理	274
コマンドライン引数	276
設定パラメータ	276
SNMPモニタリングシステムとの統合	280
Dr.Web SNMP MIB	288
Dr.Web MeshD	315
動作原理	315
コマンドライン引数	318
設定パラメータ	319



Dr.Web URL Checker	322
動作原理	323
コマンドライン引数	323
設定パラメータ	324
Dr.Web CloudD	325
動作原理	325
コマンドライン引数	326
設定パラメータ	326
Dr.Web LookupD	328
動作原理	328
コマンドライン引数	329
設定パラメータ	330
Dr.Web StatD	342
動作原理	342
コマンドライン引数	342
設定パラメータ	343
付録	345
付録A. コンピューター脅威の種類	345
付録B. コンピューター脅威の駆除	349
付録C. テクニカルサポート	351
付録D. Dr.Web for UNIX Internet Gateways設定ファイル	353
ファイル構造	353
パラメータタイプ	354
トラフィックモニタリングのルール	357
付録E. SSL証明書を生成する	375
付録F. 既知のエラー	378
付録G. 略語のリスト	429



はじめに

Dr.Web for UNIX Internet Gatewaysをお買い上げいただきありがとうございます。本製品は最先端のウイルス検出および駆除テクノロジーを活用して、さまざまなタイプのコンピューター脅威の拡散からサーバーを確実に保護します。これにより、サーバーが提供するサービスの品質を向上させることができます。

このマニュアルの目的は、GNU/LinuxファミリーのOSやFreeBSDなど、UNIXライクなOSを実行しているサーバーの管理者が、Dr.Web for UNIX Internet Gatewaysバージョン11.1をインストールしてご使用いただけるように支援することです。

ファイルパスの表記規則

ファイルとコンポーネントへの実際のパスは、OSによって異なります。本書では、ディレクトリに次の表記規則を使用しています。

- `<opt_dir>` - 主な製品ファイルがあるディレクトリ(実行ファイルとライブラリを含む)
- `<etc_dir>` - 設定ファイルとキーファイルがあるディレクトリ
- `<var_dir>` - サポートと製品の一時ファイルがあるディレクトリ

さまざまなOSの表記規則に対応する実際のパスは、以下の表に示されています。



OSの種類	表記規則	実際のパス
GNU/Linux	<code><opt_dir></code>	<code>/opt/drweb.com</code>
	<code><etc_dir></code>	<code>/etc/opt/drweb.com</code>
	<code><var_dir></code>	<code>/var/opt/drweb.com</code>
FreeBSD	<code><opt_dir></code>	<code>/usr/local/libexec/drweb.com</code>
	<code><etc_dir></code>	<code>/usr/local/etc/drweb.com</code>
	<code><var_dir></code>	<code>/var/drweb.com</code>

スペースを考慮して、例ではGNU/Linux OSのパスを使用しています。本書では、可能な場合においてすべてのOSの実際のパスが例に使用されています。



表記規則と略語

本マニュアルでは、以下の文字・記号を使用しています。

文字・記号	説明
	重要な事項や指示
	エラーの可能性や特に注意を必要とする重要な注意事項に関する警告
アンチウイルスネットワーク	新しい用語、または強調したい用語
<IP-address>	プレースホルダー
保存	ボタン、ウィンドウ、メニューアイテム、および他のプログラムインターフェース要素の名称
CTRL	キーボードのキーの名称
/home/user	ファイルやフォルダの名前、コード例
付録 A	マニュアル内の別の章への相互参照や外部 Web ページへのハイパーリンク



本マニュアルでは、(端末または端末エミュレーターで)キーボードから入力されるコマンドラインのコマンドには、コマンドプロンプト記号 \$ または # が付いています。この記号は、該当するコマンドの実行に必要な権限を表しています (UNIX 系システムの標準的表記規則に従って)。

\$ - コマンドはユーザー権限で実行できることを示します。

- スーパーユーザー (通常は *root*) 権限でコマンドを実行できることを示します。権限を昇格するには、*su* と *sudo* コマンドを使用してください。

略語のリストは、セクション [付録 G. 略語のリスト](#) にあります。



この製品について

このセクションの内容

- [機能](#)
- [Dr.Web for UNIX Internet Gatewaysのメイン機能](#)
- [Dr.Web for UNIX Internet Gatewaysの構成](#)
- [隔離への移動](#)
- [ファイルのパーミッションと権限](#)
- [動作モード](#)

機能

Dr.Web for UNIX Internet Gatewaysは、UNIX (GNU/Linux、FreeBSD) で実行されているインターネットゲートウェイやプロキシを、ウイルスや他のタイプの悪意のあるソフトウェアから保護し、さまざまなプラットフォーム向けに作成された脅威の拡散を防ぐためのものです。

主なコンポーネント (スキャンエンジンとウイルスデータベース) は、非常に効果的でリソースを節約するだけでなく、クロスプラットフォームでもあるため、Doctor Webスペシャリストはさまざまなプラットフォームをターゲットとした脅威から一般的なOSのコンピューターやモバイルデバイスを守る、信頼性の高いアンチウイルスソリューションを作成できます。現在、Doctor WebではDr.Web for UNIX Internet Gatewaysとともに、UNIXベースのOS (GNU/Linux、FreeBSDなど) とIBM OS/2、Novell NetWare、macOSおよびWindowsの両方のアンチウイルスソリューションを提供しています。さらに、Android、Symbian、BlackBerry、Windows Mobileを実行するデバイスを保護するための、他のアンチウイルス製品が開発されています。

Dr.Web for UNIX Internet Gatewaysのコンポーネントは常に更新され、ウイルスデータベース、Webリソースカテゴリーのデータベース、メールメッセージのスパムフィルタリングのルールデータベースには定期的に新しいシグネチャが追加されるため、サーバー、ワークステーション、モバイルユーザーとそのプログラムやデータに最新の保護を提供します。未知のウイルスに対する追加の保護を提供するため、スキャンエンジンとDr.Web Cloudサービスにはヒューリスティック解析が実装されており、シグネチャがデータベースにない最新の脅威に関する情報を保存します (この機能はDr.Webの一部の製品でのみ利用できます)。

Dr.Web for UNIX Internet Gatewaysのメイン機能

1. **脅威の検出と駆除。** 悪意のあるプログラム (メールファイルやブートレコードに感染するものを含むウイルス、トロイの木馬、メールワームなど) や望ましくないソフトウェア (アドウェア、ジョークプログラム、ダイアラーなど) を検索します。コンピューターの脅威の種類に関する詳細については、[付録A. コンピューター脅威の種類](#)を参照してください。

脅威の検出方法:

- **シグネチャ解析。** 既知の脅威を検出できます。
- **ヒューリスティック解析。** ウイルスデータベースに含まれていない脅威を検出できます。
- **クラウドベースの脅威検出テクノロジー。** Dr.Web Cloudサービスを使用して、新しい脅威に関する最新の情報を収集し、それをDr.Web製品に送信します。



ヒューリスティックアナライザは誤検知を引き起こす可能性があります。その結果、アナライザによって検出された脅威を含むオブジェクトは「疑わしい」と見なされます。このようなファイルを隔離し、解析のためにDoctor Webアンチウイルススラボに送信することをお勧めします。脅威を駆除する方法の詳細は、[付録B. コンピューター脅威の駆除](#)を参照してください。

ユーザーのリクエストに応じてファイルシステムをスキャンする場合、ユーザーが利用できるすべてのファイルシステムオブジェクトのフルスキャン、または指定されたオブジェクトのみ（指定された基準を満たす個別のディレクトリまたはファイル）のカスタムスキャンが可能です。さらに、システム内で現在アクティブなプロセスをサポートするボリュームと実行ファイルのブートレコードを別々にチェックすることもできます。後者の場合、脅威が検出されると、悪意のある実行ファイルを駆除するだけでなく、選択的スキャンにより実行されているすべてのプロセスが強制的に終了されます。一連の異なるアクセスレベルを持つファイルへのアクセスの必須モデルを実装するシステムでは、現在のアクセスレベルでは利用できないファイルのスキャンは特別な[自律コピー](#)モードで行うことができます。

ファイルシステムで検出された脅威を含むオブジェクトはすべて、自律コピーモードで検出された脅威を除いて、永久保存された脅威レジストリに登録されます。

Dr.Web for UNIX Internet Gatewaysに含まれている[Dr.Web Ctl](#)コマンドラインを使うと、SSHまたはTelnet経由でのリモート端末アクセスを提供するリモートネットワークホストの脅威ファイルシステムをスキャンできます。



リモートスキャンは、リモートホスト上の悪意のあるファイルや疑わしいファイルの検出にのみ使用できます。リモートホストで検出された脅威を排除するには、このホストによって直接提供される管理ツールを使用する必要があります。たとえば、ルーターやその他の「スマート」デバイスの場合は、ファームウェア更新のメカニズムを使用できます。コンピューティングマシンの場合は、コンピューティングマシンへの接続（任意でリモート端末モードを使用）とファイルシステムのそれぞれの操作（ファイルの削除または移動など）、またはコンピューティングマシンにインストールされているアンチウイルスソフトウェアの実行を介して実行できます。

- インターネットに送信されたデータの解析。ユーザーのリクエスト（つまり、Webサーバーに接続してファイルを送信しようとする試み）だけでなく、ユーザーのリクエストに応じて送信されるデータもモニタリングされます。リクエストや送信されるデータを解析するために、Dr.Web for UNIX Internet GatewaysはICAPプロトコル経由で外部フィルターとしてプロキシサーバーに接続し、ローカルネットワークユーザーのHTTP接続を処理します。さらに、SpIDer Gateコンポーネントを使用すると、組織の公開サーバーによる感染ファイルの送受信を防ぐバリア機能を実行できます（GNU/Linuxにのみこのオプションは使用できません）。この製品は、望ましくないWebサイトへのアクセスを制限するために、Dr.Web for UNIX Internet Gatewaysとともに提供され、自動的に更新されるWebリソースカテゴリーのデータベースと、システム管理者が手動で作成したホワイトリストとブラックリストを使用します。この製品はDr.Web Cloudサービスも参照して、インターネットリソースが他のDr.Web製品によって悪意のあるものとしてマークされているかどうか、情報を確認します。
- 感染したオブジェクトや疑わしいオブジェクトを確実に隔離します。サーバーのファイルシステムで検出されたそのようなオブジェクトは、システムへの害を防ぐ特別なフォルダに移動され、隔離されます。隔離へ移動されたオブジェクトは、特別なルールに従って名前が変更され、必要に応じて、要求があった場合にのみ元の場所に復元できます。

[Dr.Web ICAPD](#)コンポーネントによって検出されたHTTPプロトコルメッセージ内の脅威は、インターネットゲートウェイ上の隔離に移動されません。その代わりに、それらの読み込みと受信者への転送はブロックされ、ブロックに関するメッセージを含む特別なHTMLページがユーザーに通知されます。

- マルウェアに対する高度な保護を維持するための、スキャンエンジン、ウイルスデータベース、Webリソースカテゴリーのデータベースの自動更新。
- ウイルスイベントに関する統計の収集、脅威検出イベントのロギング。SNMPを介して検出された脅威に関する通知を、外部のモニタリングシステム、集中管理サーバー（Dr.Web for UNIX Internet Gatewaysが[集中管理モード](#)で動作している場合）、およびDr.Web Cloudに送信します。



6. 集中管理モードでの動作 (Dr.Web Enterprise Serverなどの集中管理サーバーに接続している場合、またはDr.Web AV-Deskサービスの一部として)。このモードでは、保護されたネットワーク内のコンピューターに、[統合されたセキュリティポリシー](#)を導入できます。保護されたネットワークには、企業ネットワークやプライベートネットワーク(VPN)、サービスプロバイダー(インターネットサービスプロバイダーなど)のネットワークが該当します。

Dr.Web for UNIX Internet Gatewaysの構成

Dr.Web for UNIX Internet Gatewaysは一連のコンポーネントで構成される製品であり、各コンポーネントにはそれぞれ独自の機能のセットがあります。コンポーネントはその目的に応じて次のカテゴリーに分けられます。

- **基本アンチウイルスコンポーネント**: Dr.Web for UNIX Internet Gatewaysの中核をなすコンポーネント。このカテゴリーにコンポーネントがない場合、本製品はファイル(およびその他のデータ)をスキャンできず、ウイルスやその他の脅威を検出できません。
- **脅威検索コンポーネント**: これらのコンポーネントは、Dr.Web for UNIX Internet Gatewaysの基本的なタスク(脅威や潜在的に危険なオブジェクトの検出)で使用されます。このカテゴリーに属するコンポーネントはその動作において、基本アンチウイルスコンポーネントを使用します。
- **サービスコンポーネント**: アンチウイルス保護に関する補助的な機能(アンチウイルスデータベースの更新、集中管理サーバーの接続、一般的なDr.Web for UNIX Internet Gatewaysの動作管理など)を提供します。
- **インターフェースコンポーネント**: Dr.Web for UNIX Internet Gatewaysのインターフェースを(ユーザーまたは他社製アプリケーションに)提供します。

以下は、Dr.Web for UNIX Internet Gatewaysコンポーネントのリストです。

1. 基本アンチウイルスコンポーネント

コンポーネント	説明
Dr.Web Virus-Finding Engine	<p>アンチウイルスエンジン。ウイルスと悪意のあるプログラムを検出するアルゴリズムを実装します(シグネチャ解析とヒューリスティック解析を使用)。</p> <p>Dr.Web Scanning Engineによって管理されます。</p> <p>ライブラリファイル: drweb32.dll</p> <p>ログファイルに表示される内部名: CoreEngine</p>
Dr.Web Scanning Engine	<p>スキャンエンジン。このコンポーネントはDr.Web Virus-Finding Engineとアンチウイルスデータベースを読み込みます。</p> <ul style="list-style-type: none"> ● スキャンのためにファイルの内容とブートレコードをアンチウイルスエンジンに送信します。 ● スキャン対象のファイルのキューを管理します。 ● このアクションが適用可能な脅威を修復します。 <p>Dr.Web ConfigDによって動作するか、自律的に動作できます。</p> <p>Dr.Web File CheckerおよびDr.Web Network Checkerコンポーネントで使用されます。また、Dr.Web MeshDコンポーネント(一部の動作モード)や、Dr.Web Scanning Engine APIを特別に使用する、Dr.Web for UNIX Internet Gatewaysに対して外部のアプリケーションによって使用されることもあります。</p>



コンポーネント	説明
	実行ファイル: drweb-se ログに表示される内部名: ScanEngine
ウイルスデータベース	ウイルスやその他の脅威のシグネチャ、および悪意のあるソフトウェアの検出・駆除アルゴリズムの自動的に更新されるデータベース。 Dr.Web Virus-Finding Engineによって使用され、一緒に提供されています。
Webリソースカテゴリーのデータベース	分類されたWebリソースのリストを含み、望ましくないWebサイトを識別するために使用される、自動的に更新されるデータベース。 SpIDer Gate、Dr.Web ICAPDなど、ユーザーとアプリケーションのネットワークアクティビティをスキャンするコンポーネントによって使用されます。
Dr.Web File Checker	ファイルシステムのオブジェクトをスキャンするコンポーネントと隔離マネージャー。 <ul style="list-style-type: none">• Dr.Web Scanning Engineに対してローカルのファイルシステムにあるファイルをスキャンするときに、脅威スキャンコンポーネントからタスクを受け取ります。• タスクに従ってファイルシステムのディレクトリを検索し、スキャンするファイルをDr.Web Scanning Engineに送信し、スキャンの進行状況をクライアントコンポーネントに通知します。• 感染したファイルの削除、隔離への移動と隔離からの復元、隔離ディレクトリの管理を行います。• キャッシュを構築し、最新の状態に保ちます。キャッシュには、以前にスキャンされたファイルに関する情報が含まれており、ファイルを再スキャンする周期を減らします。 ファイルシステムのオブジェクトをスキャンするコンポーネントによって使用されます。 実行ファイル: drweb-filecheck ログに表示される内部名: FileCheck
Dr.Web Network Checker	ネットワークデータスキャンエージェント。 <ul style="list-style-type: none">• スキャンエンジンへのデータの送信に使用されます。データはネットワーク経由で製品のコンポーネント(Dr.Web ClamD、SpIDer Gate、Dr.Web ICAPDなど)によって送信されます。• このコンポーネントによってDr.Web for UNIX Internet Gatewaysは分散ファイルのスキャンを管理できるようになり、リモートホストとの間でスキャン用のファイルを送受信します。そのためには、リモートホストにはUNIX OS用にインストールされ実行されているDr.Webを備えている必要があります。それによって分散スキャンモードでは、多数のスキャンタスクのあるホスト(メールサーバー、ファイルサーバー、インターネットゲートウェイなど)の負荷を減らすことで、リモートホスト間でスキャン負荷を自動的に分散できます。 スキャン用のデータを受信できるパートナーホストがネットワーク上に存在する場合、スキャンにDr.Web Network Checkerを使用するコンポーネントはローカルのDr.Web Scanning Engineを使用しない場合があります。したがって、Dr.Web Scanning Engine、Dr.Web Virus-Finding Engine、およびアンチウイルスデータベースが存在しない可能性があります。



コンポーネント	説明
	<p>セキュリティ上の理由から、ファイルはネットワーク経由でSSLを使用して転送されます。</p> <p>実行ファイル: drweb-netcheck ログに表示される内部名: NetCheck</p>
Dr.Web URL Checker	<p>URLが潜在的に危険なカテゴリーや望ましくないカテゴリーに該当するかどうかを解析するためのコンポーネント</p> <p>実行ファイル: drweb-urlcheck ログに表示される内部名: UrlCheck</p>
Dr.Web MeshD	<p>Dr.Web for UNIX Internet Gatewaysをローカルクラウドに接続するコンポーネント。Dr.Web for UNIX製品が更新およびファイルスキャンの結果を交換し、スキャンのためにファイルを相互に送信し、スキャンエンジンサービスを直接提供できるようにします。</p> <p>製品にこのコンポーネントが含まれている場合、このコンポーネントが接続されているローカルクラウドや、スキャンエンジンサービスを提供するホスト、Dr.Web Scanning Engine、Dr.Web Virus-Finding Engine、アンチウイルスデータベースが存在しない場合があります。</p> <p>実行ファイル: drweb-meshd ログに表示される内部名: MeshD</p>

2. 脅威検索コンポーネント

コンポーネント	説明
Dr.Web ICAPD	<p>ICAPをサポートするHTTPプロキシ(Squidなど)を通過するリクエストとネットワークトラフィックを解析するICAPサーバー。</p> <p>感染したファイルの送信や、インターネットリソースの望ましくないカテゴリーに該当し、システム管理者が作成したブラックリストに追加されたネットワークホストへのアクセスを防止します。外部サーバーへのアクセスが禁止されている場合や、送信されたデータに脅威が含まれている場合、プロキシサーバーは、要求されたリソースへのアクセスや感染ファイルのダウンロードが行えないことを知らせる専用のページをユーザーに返すよう指示されます。</p> <p>Dr.Web Network Checkerを使用して、プロキシサーバーから受信したデータをスキャンします。</p> <p>実行ファイル: drweb-icapd ログに表示される内部名: ICAPD</p>
SpIDer Gate	<p>ネットワークトラフィックとURLをモニタリングするためのコンポーネント。</p> <p>ネットワークからローカルホストにダウンロードされ、そこから外部ネットワークに送信されたデータの脅威をスキャンするように設計されています。またこのコンポーネントは、Webリソースの望ましくないカテゴリーや、システム管理者が作成したブラックリストに追加されたネットワークホストとの接続を阻止します。</p>



コンポーネント	説明
	<p>Dr.Web Network Checkerを使用して、受信したデータをスキャンします。</p> <div style="border: 1px solid #ccc; background-color: #e6f2e6; padding: 10px; margin: 10px 0;"> GNU/Linux OS用ディストリビューションにのみ含まれています。</div> <p>実行ファイル: drweb-gated ログに表示される内部名: GateD</p>
Dr.Web Firewall for Linux	<p>ネットワーク接続モニター。</p> <p>SpIDer Gateによって使用され、送信されたネットワークトラフィックをスキャンするためにサーバー上で動作するアプリケーションに接続ルーティングを提供します。</p> <div style="border: 1px solid #ccc; background-color: #e6f2e6; padding: 10px; margin: 10px 0;"> GNU/Linux OS用ディストリビューションにのみ含まれています。</div> <p>実行ファイル: drweb-firewall ログファイルに表示される内部名: LinuxFirewall</p>

3. サービスコンポーネント

コンポーネント	説明
Dr.Web CloudD	<p>Dr.Web Cloudとのインタラクションのためのコンポーネント。</p> <p>ユーザーが閲覧したURLと、スキャンしたファイルに関する情報をDr.Web Cloudサービスに送信して、ウイルスデータベースにまだ含まれていない脅威がないかスキャンします。</p> <p>実行ファイル: drweb-cloudd ログに表示される内部名: CloudD</p>
Dr.Web ConfigD	<p>Dr.Web for UNIX Internet Gateways設定デーモン。</p> <ul style="list-style-type: none">• 設定に応じて、他の製品のコンポーネントを起動／停止します。• コンポーネントの動作に障害が発生した場合、該当するコンポーネントを再起動します。他のコンポーネントのリクエストに応じてコンポーネントを起動します。別のコンポーネントが起動またはシャットダウンしたときに、アクティブなコンポーネントに通知します。• 現在のライセンスキーと設定に関する情報を保存し、その情報をすべてのコンポーネントに提供します。それらの情報を提供すると想定されるDr.Web for UNIX Internet Gatewaysのコンポーネントから、調整済みの設定とライセンスキーを受け取ります。ライセンスキーと設定の変更について他のコンポーネントに通知します。 <p>実行ファイル: drweb-configd ログファイルに表示される内部名: ConfigD</p>



コンポーネント	説明
Dr.Web ES Agent	<p>集中管理エージェント。集中管理モードとモバイルモードでの製品の動作を確実にものにします。</p> <ul style="list-style-type: none">製品と集中管理サーバー間の接続を提供し、ライセンスキーファイル、ウイルスデータベースとアンチウイルスエンジンの更新を受信します。Dr.Web for UNIX Internet Gatewaysに含まれるコンポーネントとそのステータス、ウイルスイベントの統計に関する情報をサーバーに送信します。 <p>実行ファイル: drweb-esagent ログに表示される内部名: ESAgent</p>
Dr.Web LookupD	<p>外部データソースからデータを取得するためのコンポーネント。</p> <p>外部データソース(ディレクトリサービス、ファイル、関連するデータベースなど)から、トラフィックモニタリングのルールで使用されるデータを取得します。</p> <p>実行ファイル: drweb-lookupd ログに表示される内部名: LookupD</p>
Dr.Web StatD	<p>Dr.Web for UNIX Internet Gatewaysのコンポーネントの動作イベントを保存するためのコンポーネント。</p> <p>製品コンポーネントのイベント(異常終了や脅威検出など)を受信して保存します。</p> <p>実行ファイル: drweb-statd ログファイルに表示される内部名: StatD</p>
Dr.Web Updater	<p>更新コンポーネント。</p> <p>ウイルスデータベース、Webリソースカテゴリーのデータベース、アンチウイルスエンジンの更新をDoctor Webのサーバーからダウンロードします。</p> <p>更新はスケジュールに従い、またユーザーの要求に応じて(Dr.Web Ctlまたは管理Webインターフェース経由で)自動的にダウンロードできます。</p> <p>実行ファイル: drweb-update ログに表示される内部名: Update</p>

4. インターフェースコンポーネント

コンポーネント	説明
Dr.Web HTTPD	<p>Dr.Web for UNIX Internet Gateways管理Webサーバー。</p> <p>Dr.Web for UNIX Internet Gatewaysコンポーネントを管理するためのカスタムHTTP APIを提供します。</p> <p>指定されたAPIは管理Webインターフェース(別途インストールが必要)によって使用されます。</p>



コンポーネント	説明
	<p>セキュリティ上の理由から、このコンポーネントはWebインターフェースへの接続にHTTPSを使用します。</p> <p>Dr.Web Network Checkerを使用して、スキャン用のデータをDr.Web Scanning Engineに送信します。</p> <hr/> <p>実行ファイル: drweb-httpd ログに表示される内部名: HTTPD</p>
Dr.Web 管理Webインターフェース	<p>管理Webインターフェース。</p> <p>このインターフェースには、ローカルホストまたはリモートホスト上の任意のブラウザからアクセスできます。このWebインターフェースにより、製品は他社製Webサーバー（Apache HTTP Serverなど）もWebminなどのリモート管理ツールも必要としません。</p> <p>このコンポーネントの機能はDr.Web HTTPDコンポーネントによって提供されます。</p>
Dr.Web Ctl	<p>コマンドラインからDr.Web for UNIX Internet Gatewaysを管理するためのツール。</p> <p>このツールによってユーザーは、ファイルスキャンの開始、隔離されたオブジェクトの表示と管理、ウイルスデータベースの更新手順の開始、Dr.Web for UNIX Internet Gatewaysと集中管理サーバー間の接続と切断、製品パラメータの表示と設定を行えるようになります。</p> <hr/> <p>実行ファイル: drweb-ctl ログに表示される内部名: Ctl</p>
Dr.Web SNMPD	<p>SNMPエージェント。</p> <p>Dr.Web for UNIX Internet GatewaysとSNMP経由の外部モニタリングシステムとの統合用に設計されています。統合することにより、製品のコンポーネントの状態を監視したり、脅威の検出と駆除に関する統計を収集したりできます。</p> <p>SNMP v2cとv3をサポートします。</p> <hr/> <p>実行ファイル: drweb-snmpd ログに表示される内部名: SNMPD</p>
Dr.Web ClamD	<p>アンチウイルスデーモンであるclamd(ClamAV®アンチウイルスのコンポーネント)のインターフェースをエミュレートするコンポーネント。</p> <p>このコンポーネントによって、ClamAV®をサポートするすべてのアプリケーションがアンチウイルススキャンにDr.Web for UNIX Internet Gatewaysを透過的に使用できるようになります。</p> <p>モードに応じてDr.Web File CheckerまたはDr.Web Network Checkerを使用して、スキャン用のデータをDr.Web Scanning Engineに送信します。</p> <hr/> <p>実行ファイル: drweb-clamd ログに表示される内部名: ClamD</p>

以下の図は、Dr.Web for UNIX Internet Gatewaysの構造とその外部アプリケーションとの動作を示しています。

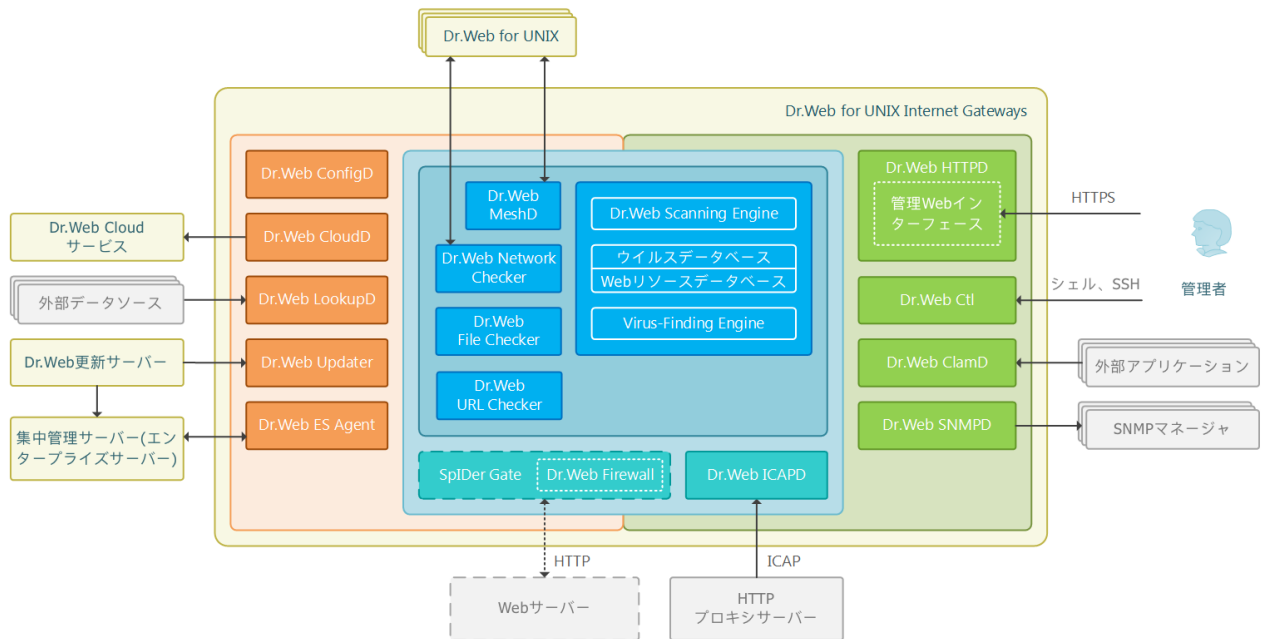


図 1. Dr.Web for UNIX Internet Gatewaysの構成

このスキームでは、次の表記法が使用されています。

	- Dr.Web for UNIX Internet Gatewaysの全体像と、ソリューションに含まれない外部のDr.Webアプリケーション。
	- Dr.Web for UNIX Internet Gatewaysの外部にあるプログラムと、それと統合されている製品。
	- 特定のアンチウイルス保護タスク(アンチウイルスデータベースの更新、集中管理サーバーへの接続、動作全体の調整など)を実行するサービスコンポーネント。
	- Dr.Web for UNIX Internet Gatewaysを管理するためのインターフェースを(ユーザーまたは他社製アプリケーションに)提供するコンポーネント。
	- アンチウイルススキャンに使用されるコンポーネント。
	- Dr.Web for UNIX Internet Gatewaysの中核をなす基本的なアンチウイルスコンポーネント。データとファイルのスキャンを実行するコンポーネントによって使用されます。

Dr.Web for UNIX Internet Gatewaysのディストリビューションと使用状況によっては、破線でマークされたコンポーネントが含まれない場合があります。

Dr.Web for UNIX Internet Gatewaysコンポーネントの詳細については、[Dr.Web for UNIX Internet Gatewaysコンポーネント](#)を参照してください。



隔離への移動

Dr.Web for UNIX Internet Gateways 11.1の隔離ディレクトリは、システムセキュリティに脅威を与え、現在修復できないファイルを分離するのに役立ちます。このような脅威は、Dr.Web for UNIX Internet Gatewaysにとって未知のもの（つまり、ヒューリスティックアナライザによってウイルスが検出されたが、ウイルスのシグネチャおよび修復方法がデータベースにないもの）または修復中にエラーを引き起こしたものになります。さらに、ユーザーが検出された脅威のリストで[アクション](#)として隔離を選択した場合や、脅威の[タイプ](#)ごとにアクションとして隔離を設定で指定した場合は、ユーザーの要求に応じてファイルを隔離できます。

隔離されたファイルの名前は特別なルールに従って変更されます。隔離されたファイルの名前を変更することで、ユーザーやアプリケーションによって特定されることを防ぎ、Dr.Web for UNIX Internet Gatewaysに備わった隔離管理ツールを回避してそれらにアクセスしようとする試みを困難にします。また、ファイルが隔離に移されると、それらを起動させる試みを防ぐために実行ビットがリセットされます。

隔離ディレクトリは以下の場所にあります。

- ユーザーのホームディレクトリ(コンピューター上に複数のユーザーアカウントが存在する場合、各ユーザーに個別の隔離ディレクトリが作成される可能性があります)
- ファイルシステムにマウントされた各論理ボリュームのルートディレクトリ

Dr.Web隔離ディレクトリの名前は常に.com.drweb.quarantineとなり、隔離[アクション](#)が適用されるまで作成されません。その際、オブジェクトを隔離するために必要なディレクトリのみが作成されます。ディレクトリを選択する際は、ファイル所有者の名前を使用します。検索は、悪意のあるオブジェクトのある場所から上の階層に向かって行われ、所有者のホームディレクトリに到達した場合、このディレクトリに作成された隔離ストレージが選択されます。そうでない場合、ファイルはボリュームのルートディレクトリ内に作成された隔離内に移されず（これはファイルシステムのルートディレクトリと同じではない場合があります）。したがって、隔離に移動された感染ファイルは常にボリューム上に配置されるため、複数のリムーバブルデータストレージやその他のボリュームがシステム内の異なる場所にマウントされている場合でも、隔離は正しく動作します。

ユーザーは、ユーティリティ[Dr.Web Ctl](#)を使用してコマンドラインから隔離コンテンツを管理できる他、[管理用 Webインターフェース](#)からも管理できます（インストールされている場合）。すべてのアクションは統合された隔離に適用されます。つまり、変更はその時点で利用可能なすべての隔離ディレクトリに影響します。



隔離されたオブジェクトに対する操作は、[有効なライセンス](#)が見つからない場合でも行うことができます。ただし、この場合、隔離されたオブジェクトは修復できません。

Dr.Web for UNIX Internet Gatewaysのすべてのアンチウイルスコンポーネントが脅威の分離に隔離を使用できるわけではありません。たとえば、Dr.Web ClamDやDr.Web ICAPD、Dr.Web MailDコンポーネント（お使いの製品には含まれていません）では使用されません。



ファイルのパーミッションと権限

ファイルシステムのオブジェクトをスキャンし、脅威を駆除するために、Dr.Web for UNIX Internet Gateways (を動作させるユーザー)は以下のパーミッションを必要とします。

アクション	必要な権限
検出されたすべての脅威を一覧にする	制限されていません。特別なパーミッションは必要ありません。
アーカイブのコンテンツを一覧表示する (破損した、または悪意のあるエレメントのみを表示する)	制限されていません。特別なパーミッションは必要ありません。
隔離へ移動する	制限されていません。その読み込みまたは書き込み権限に関係なく、ユーザーは感染したすべてのファイルを隔離できます。
脅威を削除する	ユーザーは削除するファイルに対する書き込み権限を持っている必要があります。  コンテナ(アーカイブ、メールメッセージなど)内のファイルで脅威が検出された場合は、削除アクションの代わりにコンテナの隔離への移動が実行されます。
修復する	制限されていません。アクセス権限と修復されたファイルの所有者は修復後も変わりません。  検出された脅威を削除することによって修復が可能である場合、ファイルを削除できます。
隔離からファイルを復元する	ユーザーはファイルの読み込み権限と復元先ディレクトリへの書き込み権限を持っている必要があります。
隔離からファイルを削除する	ユーザーは隔離へ移されたファイルへの書き込み権限を持っている必要があります。

スーパーユーザー (*root*) 権限でコマンドライン管理 [Dr.Web Ctl](#) ツールの動作を有効にするには、`su` コマンドを使用してユーザーを変更するか、`sudo` コマンドを使用して、他のユーザーとしてコマンドを実行できます。



Dr.Web Scanning Engine スキャンエンジンは、4GB を超えるサイズのファイルをスキャンできません (このようなファイルをスキャンしようとする、ファイルサイズが大きすぎることを示すエラーメッセージ "File is too large" が表示されます)。



動作モード

Dr.Web for UNIX Internet Gatewaysはスタンドアロンモードでも、**集中管理サーバー**によって管理されるアンチウイルスネットワークの一部としても動作できます。**集中管理モード**での動作には、追加のソフトウェアのインストールやDr.Web for UNIX Internet Gatewaysの再インストールまたは削除は必要ありません。

- **スタンドアロンモード**では、保護するコンピューターはアンチウイルスネットワークに接続されず、その操作はローカルで管理されます。このモードでは、設定ファイルとライセンスキーファイルはローカルディスクにあり、Dr.Web for UNIX Internet Gatewaysは保護するコンピューターから完全に制御されます。ウイルスデータベースの更新はDoctor Web更新サーバーから受信します。
- **集中管理モード(エンタープライズモード)**では、コンピューターの保護は集中管理サーバーによって管理されます。このモードでは、Dr.Web for UNIX Internet Gatewaysの一部の機能や設定を、アンチウイルスネットワークに対して適用される一般的な(企業の)アンチウイルス保護ポリシーに応じて変更できます。集中管理モードでの動作に使用するライセンスキーファイルは、集中管理サーバーから受け取ります。ローカルコンピューター上に保存されたデモキーファイルがある場合、それは使用されません。ウイルスイベントに関する統計は、Dr.Web for UNIX Internet Gatewaysの動作に関する情報と一緒に集中管理サーバーに送信されます。ウイルスデータベースの更新もまた、集中管理サーバーから受け取ります。
- **モバイルモード**では、Dr.Web for UNIX Internet GatewaysはDoctor Web更新サーバーから更新を受信しますが、製品の動作はローカルの設定と集中管理サーバーから受信したライセンスキーファイルで管理されます。モバイルモードに切り替えることができるのは、集中管理サーバーの設定で許可されている場合のみです。

集中管理のコンセプト

Doctor Webの集中管理ソリューションはクライアント-サーバーモデルを使用します(下図参照)。

ワークステーションとサーバーは、それらにインストールされている**ローカルのアンチウイルスコンポーネント**(以下「Dr.Web for UNIX Internet Gatewaysコンポーネント」)によって脅威から保護されます。これらコンポーネントはリモートコンピューターのアンチウイルス保護を提供し、ワークステーションと集中管理サーバーとの接続を可能にします。

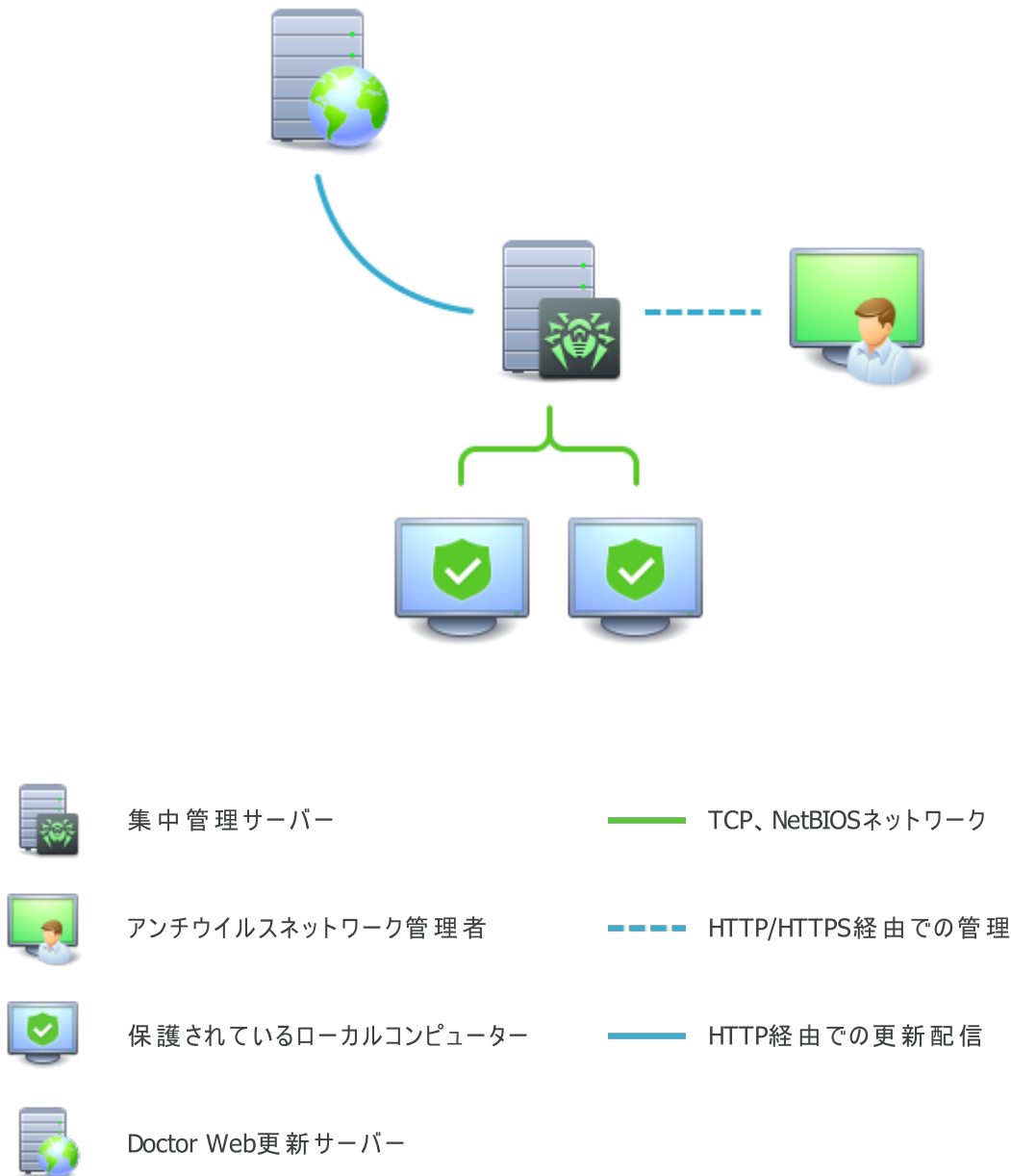


図2. アンチウイルスネットワークの論理的構造

ローカルコンピューターの更新と設定は**集中管理サーバー**から行われます。アンチウイルスネットワーク内の一連の指示やデータ、統計も集中管理サーバーを経由します。保護するコンピューターと集中管理サーバー間のトラフィック量はかなり大きくなる場合があるため、トラフィックを圧縮するオプションがソリューションに用意されています。機密データの漏洩や、保護するコンピューター上にダウンロードされたソフトウェアの置き換えを防ぐため、暗号化もサポートされています。

必要なすべての更新がDoctor Web更新サーバーから集中管理サーバーにダウンロードされます。

ローカルのアンチウイルスコンポーネントは、アンチウイルスネットワーク管理者より受け取ったコマンドに応じて集中管理サーバーから設定・管理されます。管理者は集中管理サーバーとアンチウイルスネットワークのトポロジを管理し(リモートコンピューターから集中管理サーバーへの接続を検証するなど)、必要に応じてローカルのアンチウイルスコンポーネントの動作を設定します。



ローカルのアンチウイルスコンポーネントは、他社のアンチウイルス製品、または集中管理モードでの動作をサポートしていないDr.Webのアンチウイルスソリューション(Dr.Web Anti-virusバージョン5.0など)と互換性がありません。同一のコンピューターに2つのアンチウイルスプログラムをインストールすると、システムクラッシュや重要なデータの消失を引き起こす場合があります。

集中管理モードでは、集中管理センターを使用して動作レポートをエクスポートできます。レポートはHTML、CSV、PDF、XML形式でエクスポートできます。

集中管理サーバーとの接続

Dr.Web for UNIX Internet Gatewaysは、コマンドラインベース管理ツール[Dr.Web Ctl](#)の[esconnect](#)コマンドを使用して、アンチウイルスネットワークの集中管理サーバーに接続できます。



集中管理サーバーの検証には、サーバーが使用する一意のパブリックキーに対応する証明書が使用されます。証明書ファイルを指定しない限り、Dr.Web ES Agent集中管理エージェントはデフォルトでサーバーへの接続を許可しません。証明書ファイルは、Dr.Web for UNIX File Serversを接続するサーバーが提供するアンチウイルスネットワークの管理者から入手する必要があります。

Dr.Web for UNIX Internet Gatewaysが集中管理サーバーに接続されている場合は、製品をモバイルモードに切り替えたり、集中管理モードに戻したりできます。モバイルモードのオン/オフの切り替えは、[Dr.Web ES Agent](#)コンポーネントの[MobileMode](#)設定パラメータを使用して行います。



Dr.Web for UNIX Internet Gatewaysは、集中管理サーバーの設定で許可されている場合のみ、モバイルモードに切り替えることができます。

製品をアンチウイルスネットワークから切断する

Dr.Web for UNIX Internet Gatewaysは、コマンドラインベース管理ツール[Dr.Web Ctl](#)の[esdisconnect](#)コマンドを使用して、アンチウイルスネットワークの集中管理サーバーから切断できます。



システム要件と互換性

このセクションの内容

- [システム要件](#)
- [サポートされているOSバージョンのリスト](#)
- [追加のパッケージとコンポーネント](#)
- [免責事項](#)
- [サポート対象のHTTPプロキシサーバー](#)
- [セキュリティサブシステムとの互換性](#)

システム要件

Dr.Web for UNIX Internet Gatewaysは、以下の要件を満たすコンピューターで使用できます。

コンポーネント	要件
プラットフォーム	次のアーキテクチャとコマンドシステムのプロセッサがサポートされています。 <ul style="list-style-type: none">• Intel/AMD: 32ビット (<i>IA-32</i>、<i>x86</i>)、64ビット (<i>x86-64</i>、<i>x64</i>、<i>amd64</i>)• ARM64• E2K (<i>Elbrus</i>)• IBM POWER (<i>ppc64e</i>)
RAM空き容量	500 MB以上 (1 GB以上を推奨)
ディスク空き容量	製品ディレクトリが配置されるボリュームに少なくとも2 GB
オペレーティングシステム	GNU/Linux(カーネルバージョン2.6.37以降、glibcライブラリ2.13以降、systemd 初期化システムバージョン209以降)、FreeBSD。サポートされているオペレーティングシステムのバージョンは下記を参照してください オペレーティングシステムは、PAM認証メカニズムをサポートしている必要があります
その他	次の有効なネットワーク接続： <ul style="list-style-type: none">• ウイルスデータベースとDr.Webコンポーネントの更新を可能にするための有効なインターネット接続• 集中管理モードで動作している場合は、ローカルネットワーク上の集中管理サーバーへの接続



コンポーネントDr.Web Firewall for Linuxが正しく動作するためには、以下のオプションを指定してOSカーネルが構築されている必要があります。

- `CONFIG_NETLINK_DIAG, CONFIG_INET_TCP_DIAG;`
- `CONFIG_NF_CONNTRACK_IPV4, CONFIG_NF_CONNTRACK_IPV6, CONFIG_NF_CONNTRACK_EVENTS;`
- `CONFIG_NETFILTER_NETLINK_QUEUE, CONFIG_NETFILTER_NETLINK_QUEUE_CT, CONFIG_NETFILTER_XT_MARK.`

上記のリストのうち必要なオプションの組み合わせは、使用するOSバージョンキットによって異なります。

Dr.Web for UNIX Internet Gatewaysを正しく動作させるために、以下のポートを開いてください。

目的	方向	ポート番号
更新を受け取るため	送信	80
Dr.Web Cloudサービスに接続するため	送信	2075 (TCP、UDP) 3010 (TCP) 3020 (TCP) 3030 (TCP) 3040 (TCP)

サポートされているOSバージョンのリスト

• GNU/Linux

プラットフォーム	サポートされているGNU/Linuxのバージョン
x86_64	<ul style="list-style-type: none"> • ALT 8 SP • ALT Server 9、10 • ALT Workstation 9、10 • Astra Linux Common Edition (Orel) 2.12 • Astra Linux Special Edition 1.5 (累積パッチ20201201SE15)、1.6 (累積パッチ20200722SE16)、1.7 • CentOS 7、8 • Debian 9、10、11、12 • Fedora 37、38 • GosLinux IC6 • Red Hat Enterprise Linux 7、8 • RED OS 7.2 MUROM、RED OS 7.3 MUROM • SUSE Linux Enterprise Server 12 SP3 • Ubuntu 18.04、20.04、22.04
x86	<ul style="list-style-type: none"> • ALT 8 SP • ALT Workstation 9、10 • CentOS 7



プラットフォーム	サポートされている GNU/Linux のバージョン
	<ul style="list-style-type: none">• Debian 10
ARM64	<ul style="list-style-type: none">• ALT 8 SP• ALT Server 9、10• ALT Workstation 9、10• Astra Linux Special Edition (Novorossiysk) 4.7• CentOS 7、8• Debian 11、12• Ubuntu 18.04
E2K	<ul style="list-style-type: none">• ALT 8 SP• Astra Linux Special Edition (Leningrad) 8.1 (累積パッチ 20201201SE15)• Elbrus-D MCST 1.4• GS CS Elbrus 8.32 TVGI.00311-28
ppc64el	<ul style="list-style-type: none">• CentOS 8• Ubuntu 20.04



ALT 8 SP、Astra Linux Special Edition (Novorossiysk) 4.11、Elbrus-D MCST 1.4、GosLinux IC6 では強制アクセス制御はサポートされていません。

これらの要件を満たすその他のGNU/Linuxバージョンであっても、Dr.Web for UNIX Internet Gatewaysとの完全な互換性は保証されていません。互換性の問題が発生した場合は、[テクニカルサポート](#)にお問い合わせください。

• FreeBSD

プラットフォーム	サポートされている FreeBSD のバージョン
x86	11, 12, 13
x86_64	11, 12, 13



FreeBSD OSの場合、Dr.Web for UNIX Internet Gatewaysは[ユニバーサルパッケージ](#)からのみインストールできます。

追加のパッケージとコンポーネント

Dr.Web for UNIX Internet Gatewaysでは、追加のパッケージやOSコンポーネントをインストールする必要はありません(保護されたサーバーソフトウェアを除く。以下を参照)。



[コマンドライン](#)でDr.Web for UNIX Internet Gatewaysを便利に操作するために、使用しているコマンドシェルでコマンド自動補完機能を有効にできます（無効になっている場合）。

追加のパッケージやコンポーネントのインストールで問題が発生した場合は、お使いのOSバージョンのドキュメントを参照してください。

免責事項

- SpIDer Gateは、OSにインストールされている他のファイアウォール（SUSE Linux Enterprise Server OSのShorewallやSuseFirewall2、Fedora、CentOS、Red Hat Enterprise LinuxのFirewallDなど）と競合する可能性があります。競合の兆候は、コードx109を伴うSpIDer Gateのエラーに関するメッセージ、またはコードx102を伴うDr.Web Firewall for Linuxのエラーに関するメッセージです。競合を解決する方法は、それぞれ「既知のエラー」セクションのエラー[x109](#)と[x102](#)で説明されています。
- 使用しているOSに1.4.15より前のバージョンのNetFilterが含まれている場合、SpIDer Gateは正しく動作しない可能性があります。この問題はNetFilterの内部エラーに関連しており、SpIDer Gateを無効にすると、ネットワーク接続が切断され、再確立できなくなります。この問題が発生した場合は、バージョン1.4.15以降のNetFilterを含むOSにアップグレードすることをお勧めします。この問題を解決する方法は、「既知のエラー」セクションで説明されています。

サポート対象のHTTPプロキシサーバー

HTTPプロキシサーバーとの[統合](#)には、インストールおよび設定済みのHTTPプロキシサーバーSquid 3.0以降が必要です。SquidはICAPのサポートを有効化（`--enable-icap-client`オプションを指定してコンパイル）して構築される必要があります。

[インターネットバリア](#)と[透過プロキシ](#)のモードでは、WebサーバーとHTTPプロキシサーバーに対する要件はありません。



インターネットバリアと透過プロキシモードはGNU/Linuxでのみ動作します。

セキュリティサブシステムとの互換性

デフォルトでは、Dr.Web for UNIX Internet GatewaysはSELinuxをサポートしていません。またDr.Web for UNIX Internet Gatewaysは、強制アクセスモデルを使用するGNU/Linuxシステム（たとえば、ユーザーとファイアウォールに異なる権限レベルを付与するPARSEC強制アクセスサブシステムの備わったシステムなど）では、機能が制限されたモードで動作します。

SELinuxの備わったシステム（およびその他の強制アクセスモデルを使用するシステム）にDr.Web for UNIX Internet Gatewaysをインストールする必要がある場合、Dr.Web for UNIX Internet Gatewaysの全機能が動作するように、セキュリティサブシステムの追加設定を実行する必要があります。詳細は、[セキュリティサブシステムを設定する](#)のセクションを参照してください。



ライセンス

Dr.Web for UNIX Internet Gatewaysを使用する権限は、Doctor Web社またはそのパートナーから購入したライセンスによって付与されます。ユーザー権限を特定するライセンスパラメータは、Dr.Web for UNIX Internet Gatewaysのインストール中にユーザーが同意する使用許諾契約 (<https://license.drweb.com/agreement/>を参照)に従って設定されます。ライセンスには、ユーザーとベンダーに関する情報の他、以下を含む購入した製品の使用パラメータも含まれています。

- ユーザーに対してライセンスされたコンポーネントのリスト
- Dr.Web for UNIX Internet Gatewaysのライセンス有効期間
- その他の制限(購入した製品を使用できるコンピューターの台数など)

評価目的のために、ユーザーは*試用期間*を有効化することもできます。有効化が成功すると、ユーザーは、有効化した試用期間全体にわたってDr.Web for UNIX Internet Gatewaysの全機能を使用できます。

各Doctor Web製品ライセンスには、ユーザーのコンピューターに保存されている特別なファイルに関連付けられた一意のシリアル番号があります。このファイルは、ライセンスパラメータに従ってコンポーネントの動作を制限し、*ライセンスキーファイル*と呼ばれます。試用期間が有効になると、*デモキーファイル*と呼ばれる特別なキーファイルが自動的に生成されます。

コンピューターでライセンスまたは試用期間が有効になっていない場合、Dr.Web for UNIX Internet Gatewaysコンポーネントはブロックされます。さらに、ウイルスデータベースとコンポーネントの更新プログラムをDoctor Web更新サーバーからダウンロードすることもできません。ただし、企業またはインターネットサービスプロバイダーによって管理される[アンチウイルスネットワーク](#)の一部として集中管理サーバーに接続することで、Dr.Web for UNIX Internet Gatewaysを有効化することができます。この場合、アンチウイルスの動作と更新は集中管理サーバーによって管理されます。



インストールとアンインストール

このセクションの内容

- [Dr.Web for UNIX Internet Gatewaysをインストールする](#)
- [Dr.Web for UNIX Internet Gatewaysをアップグレードする](#)
- [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#)
- [セキュリティサブシステムを設定する](#)
- 追加情報:
 - [Dr.Web for UNIX Internet Gatewaysパッケージとファイル](#)
 - [コンポーネントのカスタムインストールとアンインストール](#)

このセクションでは、Dr.Web for UNIX Internet Gatewaysバージョン11.1をインストールおよびアンインストールする方法について説明します。また、最新の更新を入手する方法や、Dr.Web for UNIX Internet Gatewaysの以前のバージョンがすでにコンピューターにインストールされている場合に新しいバージョンにアップグレードする手順も記載されています。

さらに、Dr.Web for UNIX Internet Gatewaysコンポーネントのカスタムインストールとアンインストール手順（Dr.Web for UNIX Internet Gatewaysの動作中に生じたエラーの解決方法や、機能セットを限定してインストールする方法など）、Dr.Web for UNIX Internet Gatewaysのインストールと動作に必要な可能性がある高度なセキュリティサブシステム（SELinuxなど）の設定についても確認できます。

これらの手順を進めるには、スーパーユーザー権限（*root*ユーザーの権限）が必要です。権限を昇格するには、`su`コマンドを使用してカレントユーザーを変更するか、または`sudo`コマンドを使用して、指定されたコマンドを別のユーザーの権限で実行します。



Dr.Web for UNIX Internet Gatewaysと、他社のアンチウイルス製品との互換性は保証されていません。1台のマシンに2つのアンチウイルスがインストールされることで、OSのエラーを引き起こし、重要なデータが失われる可能性があります。Dr.Web for UNIX Internet Gatewaysをインストールする前に、他社のアンチウイルス製品をコンピューターから削除することが強く推奨されます。

お使いのコンピューターに他のDr.Webアンチウイルス製品が[ユニバーサルパッケージ\(.run\)](#)からすでにインストールされていて、さらに別のDr.Webアンチウイルス製品をインストールする場合（たとえば、ユニバーサルパッケージからDr.Web for Linuxをインストールしていて、さらにDr.Web for UNIX Internet Gatewaysをインストールする場合など）、インストールされている製品のバージョンがインストールするDr.Web for UNIX Internet Gatewaysのバージョンと同じであることを確認してください。新しくインストールする製品のバージョンがインストールされている製品のものよりも新しい場合、インストール前に、インストールされているDr.Web for UNIX Internet Gatewaysを新しくインストールする製品のバージョンに[アップグレード](#)する必要があります。

FreeBSD OSの場合、Dr.Web for UNIX Internet Gatewaysは[ユニバーサルパッケージ](#)からのみインストールできます。



Dr.Web for UNIX Internet Gatewaysをインストールする

Dr.Web for UNIX Internet Gatewaysをインストールするには、以下の手順のいずれか1つを行います。

1. Doctor Webの公式Webサイトから、UNIXシステム用の[ユニバーサルパッケージ](#)を含むインストールファイルをダウンロードします。パッケージにはインストーラが含まれています（インストールプログラムはコマンドラインモード用に開発されているため、グラフィカルデスクトップモードで使用するにはターミナルエミュレーターが必要になります）。
2. Doctor Webの対応するパッケージリポジトリから[ネイティブパッケージ](#)をダウンロードします。



FreeBSD OSの場合、Dr.Web for UNIX Internet Gatewaysは[ユニバーサルパッケージ](#)からのみインストールできます。



古いバージョンのパッケージマネージャーを使用しているOS（ALT 8 SPなど）では、Dr.Web for UNIX Internet Gateways[ユニバーサルパッケージ](#)をインストールすることを推奨します。

インストール中（ユニバーサル、runパッケージからだけでなく、パッケージマネージャーを使用してネイティブパッケージからも）、インストール結果を含むメッセージがroot@localhostメールアドレスに送信されます。

上記のいずれかの方法でDr.Web for UNIX Internet Gatewaysをインストールした後、そのコンポーネントに利用可能な修正があるか、新しいDr.Web for UNIX Internet Gatewaysバージョンがリリースされている場合は、[アンインストール](#)または[更新](#)できます。必要に応じて、Dr.Web for UNIX Internet Gatewaysを正しく動作させるために、GNU/Linuxの[セキュリティサブシステムを設定](#)することもできます。個々のコンポーネントの機能に問題がある場合は、Dr.Web for UNIX Internet Gatewaysをアンインストールせずに、該当するコンポーネントの[カスタムインストールおよびアンインストール](#)を実行できます。

選択したDr.Web for UNIX Internet Gatewaysのインストール方法に関係なく、インストールが完了したら、ライセンスを有効化して、受け取ったキーファイルをインストールする必要があります。さらに、Dr.Web for UNIX Internet Gatewaysを集中管理サーバーに[接続](#)することもできます。詳細は、[ライセンス](#)を参照してください。これを行わない場合、アンチウイルス保護機能が無効になります。さらに、場合によっては、[開始](#)するのセクションで説明されているように、インストールしたDr.Web for UNIX Internet Gatewaysの基本機能をカスタマイズする必要があります。



ユニバーサルパッケージをインストールする

Dr.Web for UNIX Internet Gatewaysユニバーサルパッケージは、`drweb-<version>-av-igw-<OS>-<platform>.run`という名前のインストールファイルとして提供されます。ここで、`<OS>`はUNIXライクなOSのタイプ、`<Platform>`は、Dr.Web for UNIX Internet Gatewaysが対象としているプラットフォーム(32ビットプラットフォームはx86、64ビットプラットフォームはamd64、arm64、e2s)です。例:

```
drweb-11.1.0-av-igw-linux-x86.run
```



このセクションではこれ以降、上記のフォーマットに対応するインストールファイルの名前を `<file_name>.run`と表記します。

Dr.Web for UNIX Internet Gatewaysのコンポーネントをインストールするには以下の手順を行ってください。

1. ユニバーサルパッケージを含むインストールファイルがない場合は、Doctor Webの公式Webサイト (<https://download.drweb.com/>) からダウンロードしてください。
2. インストールファイルをコンピューターのハードディスクドライブに保存します。
3. たとえば次のコマンドを使用して、アーカイブを実行できるようにします。

```
# chmod +x <file_name>.run
```

4. 次のコマンドを使用してアーカイブを実行します。

```
# ./<file_name>.run
```

ファイルプロパティ(パーミッション)を変更するときやファイルを実行するときは、どちらの場合にもグラフィカルシェルの標準的なファイルマネージャーを使用します。これにより、アーカイブの整合性チェックが実行され、その後アーカイブファイルが一時ディレクトリに解凍され、インストールプログラムが起動されます。ユーザーがroot権限を持っていない場合、インストールプログラムはそのユーザーにrootパスワードを要求することで権限の昇格を試みます(sudoが使用されます)。この試みが失敗した場合、インストールプロセスは停止します。



ファイルシステム内の一時ディレクトリへのパスに、解凍されるファイル用の十分な空き容量がない場合、インストールプロセスが停止し、対応するメッセージが表示されます。この場合は、TMPDIRシステム環境変数の値を、十分な空き容量があるディレクトリを指すように変更し、インストールをやり直してください。--targetオプションを使用することもできます。

その後、**コマンドラインモード**用のインストーラが自動的に起動されます(グラフィカルデスクトップ環境で実行するには、ターミナルエミュレーターが必要です)。

5. インストーラの指示に従ってください。
6. 次のコマンドを実行することで、インストールプログラムをサイレントモードで起動することもできます。

```
# ./<file_name>.run -- --non-interactive
```

この場合、インストールプログラムはサイレントモードで起動され、ユーザーインターフェースなしで動作します(通常コマンドラインモードで表示されるダイアログも表示されません)。



このオプションを使用すると、Dr.Web使用許諾契約の規定に同意することになります。使用許諾契約のテキストは `/opt/drweb.com/share/doc/LICENSE` ファイルにあります。ファイル拡張子は使用許諾契約の言語を示しています。このLICENSEファイルに拡張子がない場合、Dr.Web使用許諾契約は英語で記述されています。使用許諾契約の規定に同意しない場合は、インストール後にDr.Web for UNIX Internet Gatewaysを[アンインストール](#)してください。

インストールプログラムをサイレントモードで起動するには管理者 (root) 権限が必要です。権限を昇格するには、`su`または`sudo`コマンドを使用できます。



使用しているGNU/LinuxディストリビューションにSELinuxがある場合、インストールプロセスがセキュリティサブシステムによって中断される可能性があります。このような状況になった場合は、次のコマンドでSELinuxを *Permissive*モードに設定してください。

```
# setenforce 0
```

次に、インストーラを再起動させます。インストールが完了した後、製品コンポーネントが正常に動作するよう、SELinuxの[セキュリティポリシー](#)を設定します。

`<opt_dir>`、`<etc_dir>`、`<var_dir>`の表記規則の詳細は、[はじめに](#)を参照してください。

インストールプロセスが完了すると、解凍されたインストールファイルがすべて削除されます。



`<file_name>.run`ファイル(インストール元のファイル)を保存しておくことを推奨します。これにより、バージョンの更新を必要とせずにDr.Web for UNIX Internet Gatewaysやそのコンポーネントを再インストールすることが可能になります。

コマンドラインからインストールする

コマンドラインベースのインストールプログラムを起動すると、製品をインストールするように促すメッセージが表示されます。

1. インストールを開始するには、「Do you want to continue?」の質問に対してYesまたはYを入力します。インストーラを終了するには、NoまたはNを入力します。この場合、インストールはキャンセルされます。
2. その後、画面に表示されているDr.Web使用許諾契約の規約を確認する必要があります。ENTERキーを押してテキストを1行ずつ下にスクロールするか、またはSPACEキーを押してテキストを1画面ずつ下にスクロールします。



使用許諾契約を上にもスクロールするオプションはありません。

3. 使用許諾契約のテキストを読んだ後、規約に同意するように求められます。使用許諾契約に同意する場合は、YesまたはYを入力します。同意しない場合は、NoまたはNを入力します。後者の場合、インストーラは終了します。
4. 使用許諾契約の規約に同意すると、インストールが自動的に開始されます。手順の実行中、インストールされるDr.Webコンポーネントの一覧を含むインストールプロセスに関する情報が画面に表示されます。



5. インストールが正常に完了すると、Dr.Web for UNIX Internet Gatewaysの動作を管理する方法を通知するメッセージが表示されます。

エラーが発生した場合は、エラーについて説明するメッセージが画面に表示された後、インストーラが終了します。インストールがエラーによって失敗した場合、エラーの原因を取り除き、インストールを再度開始してください。

リポジトリからインストールする

Dr.Web for UNIX Internet Gatewaysのネイティブパッケージは<https://repo.drweb.com/>にあるDr.Webの公式リポジトリに保存されています。お使いのOSのパッケージマネージャーが使用するリポジトリのリストにDr.Webリポジトリを追加すると、OSのリポジトリから他のプログラムをインストールするのと同じようにネイティブパッケージから製品をインストールできます。必要な依存関係は自動的に解決されます。



以下で説明するコマンド(リポジトリの追加、デジタル署名キーのインポート、パッケージのインストールと削除に使用するコマンド)はすべて、スーパーユーザー(root)権限で実行する必要があります。この権限を昇格するには、(現在のユーザーを変更する)suコマンド、または(他のユーザーの権限で指定したコマンドを実行する)sudoコマンドを使用します。

FreeBSD OSの場合、Dr.Web for UNIX Internet Gatewaysは[ユニバーサルパッケージ](#)からのみインストールできます。

以下のOS(パッケージマネージャー)の手順を参照してください。

- [Debian、Mint、Ubuntu \(apt\)](#)
- [ALT Linux、PCLinuxOS \(apt-rpm\)](#)
- [Mageia、OpenMandriva Lx \(urpmi\)](#)
- [Red Hat Enterprise Linux、Fedora、CentOS \(yum、dnf\)](#)
- [SUSE Linux \(zypper\)](#)

Debian、Mint、Ubuntu (apt)

リポジトリから**Dr.Web for UNIX Internet Gateways**をインストールする

1. これらOS用のリポジトリはDoctor Webによって電子署名されています。リポジトリにアクセスするには、以下のコマンドを実行することで、デジタル署名キーをインポートし、パッケージマネージャストレージに追加します。

```
# apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys  
8C42FC58D8752769
```

2. リポジトリを追加するには、`/etc/apt/sources.list`ファイルに以下のラインを追加します。

```
deb http://repo.drweb.com/drweb/debian 11.1 non-free
```



1および2の項目は、リポジトリから特別なDEBパッケージ (<https://repo.drweb.com/drweb/drweb-repo11.1.deb>) をダウンロードしてインストールすることも実行できます。

3. リポジトリからDr.Web for UNIX Internet Gatewaysをインストールするには、以下のコマンドを使用します。

```
# apt-get update
# apt-get install drweb-internet-gateways
```

代替のパッケージマネージャー (Synapticまたはaptitudeなど) を使用して製品をインストールすることもできます。パッケージの競合が発生した場合は、それを解決するためにaptitudeなどの代替のマネージャーを使用することが推奨されます。

ALT Linux、PCLinuxOS (apt-rpm)

リポジトリからDr.Web for UNIX Internet Gatewaysをインストールする

1. リポジトリを追加するには、`/etc/apt/sources.list`ファイルに以下のラインを追加します。

```
rpm http://repo.drweb.com/drweb/altlinux 11.1/ <arch> drweb
```

ここで、`<arch>`は、次に示すパッケージのアーキテクチャを表します。

- 32-bitバージョン: `i386`
- AMD64アーキテクチャ: `x86_64`
- ARM64アーキテクチャ: `aarch64`
- E2Kアーキテクチャ: `e2s`

2. リポジトリからDr.Web for UNIX Internet Gatewaysをインストールするには、以下のコマンドを使用します。

```
# apt-get update
# apt-get install drweb-internet-gateways
```

代替のパッケージマネージャー (Synapticまたはaptitudeなど) を使用して製品をインストールすることもできます。

Mageia、OpenMandriva Lx (urpmi)

リポジトリからDr.Web for UNIX Internet Gatewaysをインストールする

1. 以下のコマンドを使用してリポジトリを接続します。

```
# urpmi.addmedia drweb https://repo.drweb.com/drweb/linux/11.1/ <arch>/
```

ここで、`<arch>`は、次に示すパッケージのアーキテクチャを表します。

- 32-bitバージョン: `i386`



- 64-bitバージョン: x86_64
2. リポジトリからDr.Web for UNIX Internet Gatewaysをインストールするには、以下のコマンドを使用します。

```
# urpmi drweb-internet-gateways
```

代替のパッケージマネージャー (rpm-drake など) を使用して製品をインストールすることもできます。

Red Hat Enterprise Linux、Fedora、CentOS (yum、dnf)

リポジトリからDr.Web for UNIX Internet Gatewaysをインストールする

1. 以下のコンテンツが含まれたdrweb.repoファイルを/etc/yum.repos.dディレクトリに追加します。

```
[drweb]
name=DrWeb-11.1
baseurl=https://repo.drweb.com/drweb/linux/11.1/$basearch/
gpgcheck=1
enabled=1
gpgkey=https://repo.drweb.com/drweb/drweb.key
```



echoなどのコマンドを使用して上記のコンテンツをファイルにロギングし、出力をリダイレクトする場合は、\$記号をエスケープする必要があります(\<\$)。

項目1は、リポジトリから特別なRPMパッケージ(<https://repo.drweb.com/drweb/drweb-repo11.1.rpm>)をダウンロードしてインストールすることも実行できます。

2. リポジトリからDr.Web for UNIX Internet Gatewaysをインストールするには、以下のコマンドを使用します。

```
# yum install drweb-internet-gateways
```

Fedoraのバージョン22以降では、マネージャーyumの代わりにdnfを使用することが推奨されます。例:

```
# dnf install drweb-internet-gateways
```

代替のパッケージマネージャー (PackageKitまたはYumexなど) を使用して製品をインストールすることもできます。

SUSE Linux (zypper)

リポジトリからDr.Web for UNIX Internet Gatewaysをインストールする

1. リポジトリを追加するには、以下のコマンドを使用します。

```
# zypper ar https://repo.drweb.com/drweb/linux/11.1/\<$basearch/ drweb
```



2. リポジトリからDr.Web for UNIX Internet Gatewaysをインストールするには、以下のコマンドを使用します。

```
# zypper refresh
# zypper install drweb-internet-gateways
```

代替のパッケージマネージャー (YaST など) を使用して製品をインストールすることもできます。

Dr.Web for UNIX Internet Gatewaysをアップグレードする

Dr.Web for UNIX Internet Gatewaysには2つの更新モードがあります。

1. Dr.Web for UNIX Internet Gatewaysの現在のバージョンのサポート期間にリリースされた[パッケージやコンポーネントの更新を入手する](#)。通常、このような更新ではエラー修正やコンポーネント機能の軽微な改良が行われています。
2. [Dr.Web for UNIX Internet Gatewaysの新しいバージョンにアップグレードする](#)。このアップグレードオプションは、お使いのDr.Web for UNIX Internet Gatewaysの新しいバージョンをDoctor Webがリリースし、それに新しい機能が備わっている場合に使用されます。



保護されたサーバーでインターネットにアクセスできない場合でも、Dr.Web for UNIX Internet Gatewaysでは[ウイルスデータベースやアンチウイルスエンジンを更新](#)できます。

パッケージとコンポーネントを更新する

[該当するセクション](#)に記載されている方法を使用してDr.Web for UNIX Internet Gatewaysをインストールすると、パッケージマネージャーは自動的にDr.Web[パッケージ](#)リポジトリに接続します。

- インストールが[ユニバーサルパッケージ](#) (ファイル: run) から実行され、システムでDEBパッケージが使用されていたり (たとえば、Debian、Mint、UbuntuなどのOS)、OSにパッケージマネージャーがない場合 (FreeBSD)、Dr.Webパッケージの動作には、それぞれのバージョンのパッケージマネージャーzypperが使用されます。これはDr.Web for UNIX Internet Gatewaysのインストール時に自動的にインストールされます。

このマネージャーが含まれる、更新されたDr.Webパッケージを入手してインストールするには、`<opt_dir>/bin`ディレクトリ (GNU/Linuxの場合は `/opt/drweb.com/bin`) に移動し、次のコマンドを実行します。

```
# ./zypper refresh
# ./zypper update
```



FreeBSD OS 11.x for amd64では、更新にzypperマネージャーを使用すると、リポジトリの更新エラーが発生する場合があります。この場合は `compat10x-amd64` サポートパッケージをインストールして、再試行してください。

パッケージをインストールするには、次のコマンドを使用します。

```
# pkg install compat10x-amd64
```



- それ以外の場合は、お使いのOSで使用されているパッケージマネージャーの更新コマンドを使用します。次に例を示します。
 - Red Hat Enterprise LinuxとCentOSではyumコマンドを使用します。
 - Fedoraではyumまたはdnfコマンドを使用します。
 - SUSE Linuxではzypperコマンドを使用します。
 - MageiaとOpenMandriva Lxではurpmiコマンドを使用します。
 - Alt Linux、PCLinuxOS、Debian、Mint、Ubuntuではapt-getコマンドを使用します。

また、お使いのOS用に開発された別のパッケージマネージャーを使用することもできます。必要に応じて、使用しているパッケージマネージャーのマニュアルを参照してください。

新しいバージョンのDr.Web for UNIX Internet Gatewaysがリリースされると、そのコンポーネントを含むパッケージは、新しいバージョンに対応するDr.Webリポジトリのセクションに配置されます。この場合、パッケージマネージャーを新しいDr.Webリポジトリセクションに切り替えて更新する必要があります([新しい製品バージョンにアップグレードする](#)を参照)。

新しい製品バージョンにアップグレードする

このセクションの内容

- [注意事項](#)
- [アップグレードのためにユニバーサルパッケージをインストールする](#)
- [リポジトリからアップグレードする](#)
- [キーファイルの転送](#)
- [集中管理サーバーとの接続を復元する](#)

注意事項



新しいバージョンにアップグレードする前に、サーバーが新しいバージョンのシステム要件を満たしていることを確認してください。これには、必要なプログラムがインストールされていることを含みます。

お使いのバージョンのDr.Web for UNIX Internet Gatewaysは、製品のインストール時と同じ方法でアップグレードする必要があります。

- Dr.Web for UNIX Internet Gatewaysの現在のバージョンがリポジトリからインストールされている場合、アップグレードではリポジトリからのプログラムパッケージを更新する必要があります。
- Dr.Web for UNIX Internet Gatewaysの現在のバージョンがユニバーサルパッケージからインストールされている場合、Dr.Web for UNIX Internet Gatewaysをアップグレードするには、新しいバージョンの製品を含んでいる別のユニバーサルパッケージをインストールする必要があります。



製品バージョンのインストール方法を特定するには、Dr.Web for UNIX Internet Gatewaysの実行可能ディレクトリに`uninst.sh`のアンインストールスクリプトが存在するかどうかを確認します。存在する場合、現在のバージョンはユニバーサルパッケージからインストールされています。存在しない場合には、リポジトリからインストールされています。

FreeBSD OSの場合、Dr.Web for UNIX Internet Gatewaysは [ユニバーサルパッケージ](#)からのみインストールできます。

インストールに使用した方法でDr.Web for UNIX Internet Gatewaysを更新できない場合は、現在のバージョンのDr.Web for UNIX Internet Gatewaysをアンインストールしてから、何らかの方法で新しいバージョンをインストールしてください。以前のバージョンのDr.Web for UNIX Internet Gatewaysのインストールおよびアンインストール手順は、バージョン11.1向けの本マニュアルにある[インストール](#)および[アンインストール](#)と同じです。追加情報については、最新バージョンのDr.Web for UNIX Internet Gatewaysのユーザーマニュアルを参照してください。

Dr.Web for UNIX Internet Gatewaysが[集中管理](#)モードで動作している場合は、集中管理サーバーのアドレスを記録することをお勧めします。たとえば、バージョン6.0.2よりも新しいDr.Web for UNIX Internet Gatewaysで集中管理サーバーのアドレスを確認するには、次のコマンドを使用できます。

```
$ drweb-ctl appinfo
```

このコマンドの出力には、次の行があります。

```
ESAgent; <PID>; RUNNING 1; Connected <address>, on-line
```

`<address>`の部分を保存します(`tcp://<IP address>:<port>`のようになっています。例：`tcp://10.20.30.40:1234`)。また、サーバー証明書ファイルを保存することをお勧めします。

現在使用している接続パラメータを調べる際に問題が発生した場合は、現在お使いのバージョンのDr.Web for UNIX Internet Gatewaysの管理者マニュアルをご確認いただき、アンチウイルスネットワーク管理者までお問い合わせください。

アップグレードのためにユニバーサルパッケージをインストールする

[ユニバーサルパッケージ](#)からDr.Web for UNIX Internet Gateways 11.1をインストールします。自動更新が不可能な場合は、新しいバージョンのインストール中に、コンピューターにインストールされているDr.Web for UNIX Internet Gatewaysの古いバージョンのコンポーネントを自動的に削除するメッセージが表示されます。



更新中に、インストールされたバージョンのDr.Web for UNIX Internet Gatewaysを削除する必要があり、Dr.Webの複数のサーバー製品（ファイルサーバー用、メールサーバー用、インターネットゲートウェイ用の製品など）がお使いのサーバーと一緒にインストールされている場合、アップグレードされない他のサーバー製品を完全に機能させるために（すなわち、ファイルサーバー用およびメールサーバー用の製品を維持するために）、削除対象として以下のパッケージのみを選択する必要があります。

- `drweb-internet-gateways-doc`
- `drweb-icapd.`

リポジトリからアップグレードする



Dr.Webバージョン6.0.2の複数のサーバー製品がお使いのサーバーと一緒にインストールされている場合（ファイルサーバー用製品、メールサーバー用製品、インターネットゲートウェイ用製品がインストールされている場合など）、Dr.Web for UNIX Internet Gateways 6.0.2をリポジトリからバージョン11.1にアップグレードすることはできません。この場合は、新しいバージョンのDr.Web for UNIX Internet Gatewaysを別のマシンにインストールしてください。

Doctor Webのリポジトリからインストールされた現在のバージョンのDr.Web for UNIX Internet Gatewaysをアップグレードする

Doctor Webリポジトリからインストールされた現在のバージョンのDr.Web for UNIX Internet Gatewaysをアップグレードするには、必要なパッケージのタイプに応じて、次のいずれかの操作を行います。

• RPMパッケージ(yum、dnf)

1. リポジトリを変更します（現在のバージョンのパッケージリポジトリから11.1パッケージリポジトリへ）。



[リポジトリからインストールする](#)セクションで、11.1パッケージが保存されているリポジトリの名前を確認できます。リポジトリの変更方法の詳細については、お使いのOSディストリビューションのヘルプガイドを参照してください。

2. 次のコマンドを使用して新しいバージョンをインストールします。

```
# yum update
```

または、マネージャーdnfを使用している場合（バージョン22以降のFedoraなど）は、以下のコマンドを使用します。

```
# dnf update
```



パッケージの更新中にエラーが発生した場合は、Dr.Web for UNIX Internet Gatewaysをアンインストールして、再度インストールしてください。必要に応じて、セクション[リポジトリからインストールしたDr.Web for UNIX Internet Gatewaysをアンインストールする](#)および[リポジトリからインストールする](#)（使用しているOSおよびパッケージマネージャーの項目）を参照してください。

• DEBパッケージ(apt-get)

1. リポジトリを変更します（現在のバージョンのパッケージリポジトリから11.1パッケージリポジトリへ）。
2. 次のコマンドを入力して、Dr.Web for UNIX Internet Gatewaysパッケージをアップグレードします。

```
# apt-get update  
# apt-get dist-upgrade
```



Ubuntu 14.04(64ビット版)OSの場合、`apt-get dist-upgrade`コマンドが失敗する場合があります。この場合は[aptitude](#)パッケージマネージャーを使用してください（製品をアップグレードするには、`aptitude dist-upgrade`コマンドを実行します）。



キーファイルの転送

Dr.Web for UNIX Internet Gatewaysをアップグレードするために選択した方法に関係なく、現在のライセンスキーファイル(お持ちの場合)は自動的に転送され、新しいバージョンに必要な正しい場所にインストールされます。



キーファイルの自動インストール中に問題が発生した場合は、[手動でインストール](#)できます。

有効なライセンスキーファイルを紛失した場合は、[テクニカルサポート](#)に連絡してください。

集中管理サーバーとの接続を復元する

可能であれば、アップグレード後に集中管理サーバーへの接続が自動的に復元されます(アップグレード前に製品が集中管理サーバーに接続されていた場合)。接続が自動的に復元されなかった場合は、アップグレードしたDr.Web for UNIX Internet Gatewaysのアンチウイルスネットワークへの接続を再度確立するために、次のコマンドを実行します。

```
$ drweb-ctl esconnect <address> --Certificate <path to the certificate file>
```

接続処理に問題が発生した場合は、アンチウイルスネットワークの管理者までお問い合わせください。

インターネットに接続せずにデータベースを更新する

インターネット接続がブロックまたは制限されている高度に安全な環境では、オフラインでウイルスデータベースを更新できます。その場合は、インターネットに接続されているコンピューターに更新をダウンロードし、USBドライブまたはローカルネットワーク共有にコピーしてから、別の(インターネットに接続されていない)コンピューターにインストールする必要があります。更新手順はコマンドラインから実行する必要があります。

更新を入手する

1. インターネットに接続されているコンピューターで次のコマンドを実行します。

```
$ drweb-ctl update --Path <a path to a directory to store updates>
```

2. ダウンロードした更新をUSBドライブまたはローカルネットワーク共有にコピーします。
3. 更新するコンピューターにローカルネットワーク共有またはリムーバブルドライブをマウントします。USBドライブから更新する場合は、次のコマンドを実行します。

```
# mkdir /mnt/usb  
# mount <a path to the device> /mnt/usb
```

4. 次のコマンドで更新を適用します。

```
$ drweb-ctl update --From /mnt/usb
```




Dr.Web for UNIX Internet Gatewaysをアンインストールする

Dr.Web for UNIX Internet Gatewaysをインストールした方法に応じて、次のいずれかの方法で製品を削除できます。

1. [アンインストーラを起動して](#)、ユニバーサルパッケージをアンインストールする。
2. システムのパッケージマネージャーを使用して、Doctor Webのリポジトリからインストールした[パッケージをアンインストールする](#)。

ユニバーサルパッケージをアンインストールする

UNIXシステム向けの[ユニバーサルパッケージ](#)からインストールされたDr.Web for UNIX Internet Gatewaysは、コマンドラインからアンインストールできます（このオプションでは、グラフィカルデスクトップ環境を使用している場合、端末エミュレーターが必要です）。



アンインストールツールはDr.Web for UNIX Internet Gatewaysだけでなく、コンピューターにインストールされている他のすべてのDr.Web製品をアンインストールします。

Dr.Web for UNIX Internet Gateways以外の他のDr.Web製品がコンピューターにインストールされている状況でDr.Web for UNIX Internet Gatewaysのみを削除するには、自動削除ツールを実行する代わりに[コンポーネントのカスタムインストールとアンインストール](#)の手順を使用します。

コマンドラインからDr.Web for UNIX Internet Gatewaysをアンインストールする

アンインストールツールは、<opt_dir>/binディレクトリ(GNU/Linuxでは/opt/drweb.com/bin)にあるuninst.shスクリプトによって起動されます。Dr.Web for UNIX Internet Gatewaysのアンインストール手順については、[コマンドラインからアンインストールする](#)のセクションで説明されています。

次のコマンドを実行することで、アンインストールツールをサイレントモードで起動することもできます。

```
# env DRWEB_NON_INTERACTIVE=yes /opt/drweb.com/bin/uninst.sh
```

この場合、アンインストールツールはサイレントモードで実行され、ユーザーインターフェースなしで動作します（コマンドラインモードのプログラムダイアログを含みます）。



アンインストールツールをサイレントモードで起動するにはroot権限が必要です。権限を昇格するには、suまたはsudoコマンドを使用できます。



古いバージョンのパッケージマネージャーを使用しているOS (ALT 8 SPなど) でユニバーサルパッケージをアンインストールする場合、次のようなメッセージが表示されることがあります。

```
/etc/init.d/drweb-configd: No such or directory
```

これらのメッセージは、システムの機能に影響を与えるものではありません。アンインストールは正しく行われています。

コマンドラインからアンインストールする

コマンドラインベースのアンインストールプログラムが起動すると、製品を削除するメッセージがコマンドラインに表示されます。

1. 削除を開始するには、「Do you want to continue?」リクエストに対して「Yes」または「Y」を入力します。アンインストールを終了するには、「No」または「N」と入力します。この場合、Dr.Web製品の削除はキャンセルされます。
2. アンインストールを確定すると、インストールされているすべてのDr.Web製品の自動アンインストールが開始されます。この手順の間、削除のプロセスに関する情報が画面に表示され、アンインストールログに記録されます。
3. プロセスが完了すると、アンインストールプログラムは自動的に終了します。

リポジトリからインストールしたDr.Web for UNIX Internet Gatewaysをアンインストールする

以下のOS (パッケージマネージャー) の手順を参照してください。

- [Debian、Mint、Ubuntu \(apt\)](#)
- [ALT Linux、PCLinuxOS \(apt-rpm\)](#)
- [Mageia、OpenMandriva Lx \(urpmi\)](#)
- [Red Hat Enterprise Linux、Fedora、CentOS \(yum、dnf\)](#)
- [SUSE Linux \(zypper\)](#)



以下に記載される、パッケージのアンインストールに使用されるコマンドはスーパーユーザー (root) 権限で実行する必要があります。権限を昇格するには、suコマンド (カレントユーザーを変更する) または sudoコマンド (指定されたコマンドを別のユーザーの権限で実行する) を使用します。



Debian、Mint、Ubuntu (apt)

Dr.Web for UNIX Internet Gatewaysのルートメタパッケージをまとめてアンインストールするには、次のコマンドを入力します。

```
# apt-get remove drweb-internet-gateways
```

ルートのメタパッケージをすべての依存ファイルと一緒にアンインストールする必要がある場合は、次のように`--autoremove`オプションを使用します。

```
# apt-get remove drweb-internet-gateways --autoremove
```

不要になったすべてのパッケージを自動的にアンインストールするには、次のコマンドを入力します。

```
# apt-get autoremove
```



アンインストールの特別な側面

1. 最初のコマンドのケースでは、`drweb-internet-gateways`パッケージのみをアンインストールします。このパッケージの依存関係を解決するのに自動的にインストールされた可能性のある他のパッケージはシステムに残ります。
2. 2番目のコマンドのケースでは、`drweb-internet-gateways`パッケージと、他のパッケージの依存関係を解決するために自動的にインストールされ、依存パッケージのアンインストールなどにより不要になったすべてのパッケージをアンインストールします。
3. 3番目のコマンドのケースでは、他のパッケージの依存関係を解決するために自動的にインストールされ、依存パッケージのアンインストールなどにより不要になったパッケージをすべてアンインストールします。
このコマンドはDr.Web for UNIX Internet Gatewaysのパッケージだけでなく、使用されていないすべてのパッケージをアンインストールします。

代替のマネージャー (Synapticまたはaptitudeなど) を使用してパッケージをアンインストールすることもできます。

ALT Linux、PCLinuxOS (apt-rpm)

この場合、Dr.Web for UNIX Internet Gatewaysのアンインストールは、DebianおよびUbuntu上でのアンインストールと同じです ([上記](#)を参照)。

代替のマネージャー (Synapticまたはaptitudeなど) を使用してパッケージをアンインストールすることもできます。



ALT 8 SPでは、ユニバーサルパッケージのアンインストール時に次のようなメッセージが表示されることがあります。

```
/etc/init.d/drweb-configd: No such or directory
```

これらのメッセージは、システムの機能に影響を与えるものではありません。アンインストールは正しく行われています。

Mageia、OpenMandriva Lx(urpme)

Dr.Web for UNIX Internet Gatewaysをアンインストールするには、次のコマンドを入力します。

```
# urpme drweb-internet-gateways
```

不要になったすべてのパッケージを自動的にアンインストールするには、次のコマンドを入力します。

```
# urpme --auto-orphans drweb-internet-gateways
```



アンインストールの特別な側面

1. 最初のコマンドのケースでは、`drweb-internet-gateways`パッケージのみをアンインストールします。このパッケージの依存関係を解決するのに自動的にインストールされた可能性のある他のパッケージはシステムに残ります。
2. 2番目のコマンドのケースでは、`drweb-internet-gateways`パッケージと、他のパッケージの依存関係を解決するために自動的にインストールされ、依存パッケージのアンインストールなどにより不要になったすべてのパッケージをアンインストールします。このコマンドはDr.Web for UNIX Internet Gatewaysのパッケージだけでなく、使用されていないすべてのパッケージをアンインストールします。

代替のマネージャー(`rpm-drake`など)を使用してパッケージをアンインストールすることもできます。

Red Hat Enterprise Linux、Fedora、CentOS(yum、dnf)

インストールされているすべてのDr.Webパッケージをアンインストールするには、次のコマンドを入力します(一部のOSでは「*」記号を「*」としてエスケープする必要があります)。

```
# yum remove drweb*
```

Fedoraのバージョン22以降では、マネージャー`yum`の代わりに`dnf`を使用することが推奨されます。例:

```
# dnf remove drweb*
```



アンインストールの特別な側面

これらのコマンドは、名前が「drweb」(Dr.Web製品名の標準的接頭辞)で始まるすべてのパッケージをアンインストールします。
これらのコマンドはDr.Web for UNIX Internet Gatewaysのパッケージだけでなく、この接頭辞を持つパッケージをすべてアンインストールします。

代替のマネージャー(PackageKitまたはYumexなど)を使用してパッケージをアンインストールすることもできます。

SUSE Linux(zypper)

Dr.Web for UNIX Internet Gatewaysをアンインストールするには、次のコマンドを入力します。

```
# zypper remove drweb-internet-gateways
```

インストールされているすべてのDr.Webパッケージをアンインストールするには、次のコマンドを入力します(一部のOSでは「*」記号を「*」としてエスケープする必要があります)。

```
# zypper remove drweb*
```



アンインストールの特別な側面

1. 最初のコマンドのケースでは、drweb-internet-gatewaysパッケージのみをアンインストールします。このパッケージの依存関係を解決するのに自動的にインストールされた可能性のある他のパッケージはシステムに残ります。
2. 2番目のコマンドのケースでは、drweb-internet-gatewaysパッケージと、他のパッケージの依存関係を解決するために自動的にインストールされ、依存パッケージのアンインストールなどにより不要になったすべてのパッケージをアンインストールします。

代替のマネージャー(YaSTなど)を使用してパッケージをアンインストールすることもできます。

追加情報

Dr.Web for UNIX Internet Gatewaysパッケージとファイル

パッケージ

Dr.Web for UNIX Internet Gatewaysは以下のパッケージで構成されています。

パッケージ	コンテンツ
drweb-bases	ウイルスデータベースファイル
drweb-boost	ブーストライブラリ



パッケージ	コンテンツ
drweb-clamd	Dr.Web ClamDコンポーネントのファイル
drweb-cloudd	Dr.Web CloudDコンポーネントのファイル
drweb-common	メインの設定ファイル - drweb.ini、メインライブラリ、ドキュメント、Dr.Web for UNIX Internet Gatewaysディレクトリの階層、製品設定とシステム環境に関する情報を収集するためのユーティリティ。 このパッケージのインストール中に、drwebという名前のユーザーとdrwebという名前のグループが作成されます。
drweb-configd	Dr.Web ConfigDのファイル
drweb-configure	Dr.Web for UNIX Internet Gateways設定用の補助ツールのファイル
drweb-ctl	Dr.Web Ctlのファイル
drweb-documentation	HTMLフォーマットのDr.Web for UNIX製品ドキュメントファイル
drweb-dws	Webリソースカテゴリーのデータベースのファイル
drweb-engine	Dr.Web Virus-Finding Engineスキャンエンジンのファイル
drweb-esagent	Dr.Web ES Agentコンポーネントのファイル
drweb-filecheck	Dr.Web File Checkerコンポーネントのファイル
drweb-internet-gateways-doc	PDFドキュメント
drweb-internet-gateways	Dr.Web for UNIX Internet Gatewaysのルートメタパッケージ
drweb-gated	SpIDer Gateコンポーネントのファイル
drweb-firewall	Dr.Web Firewall for Linuxコンポーネントのファイル
drweb-httpd	Dr.Web HTTPDコンポーネントと管理Webインターフェース(メタパッケージ)のファイル
drweb-httpd-bin	Dr.Web HTTPDコンポーネントのファイル
drweb-httpd-webconsole	管理Webインターフェースのファイル
drweb-icu	Unicodeサポートとインターナショナルライゼーションのためのライブラリ
drweb-icapd	Dr.Web ICAPDコンポーネントのファイル
drweb-libs	メインライブラリファイル
drweb-lookupd	Dr.Web LookupDコンポーネントのファイル



パッケージ	コンテンツ
drweb-lua	ネットワーク接続監視用に設計されたDr.Web for UNIX Internet Gatewaysコンポーネントによって使用されるLuaインタプリタのファイル
drweb-netcheck	Dr.Web Network Checkerコンポーネントのファイル
drweb-openssl	OpenSSLライブラリ
drweb-protobuf	Google Protobufライブラリ
drweb-se	Dr.Web Scanning Engineコンポーネントのファイル
drweb-snmpd	Dr.Web SNMPDコンポーネントのファイル
drweb-update	Dr.Web Updaterコンポーネントのファイル

セクション[コンポーネントのカスタムインストールとアンインストール](#)には、Dr.Web for UNIX Internet Gatewaysの典型的なタスクに対する解決策を提供するカスタムインストール用の典型的なコンポーネントセットがあります。

ファイル

Dr.Web for UNIX Internet Gatewaysのインストール後、その構成ファイルはファイルシステムの/opt、/etc、/varディレクトリに置かれます。

Dr.Web for UNIX Internet Gatewaysディレクトリの構造：

ディレクトリ	コンテンツ
<ul style="list-style-type: none">• GNU/Linuxの場合： /etc/init.d/• FreeBSDの場合： /usr/local/etc/rc.d/	Dr.Web ConfigDデーモン用のdrweb-configdスクリプト
<etc_dir>	drweb.ini設定ファイルとdrweb32.keyキーファイル。また、次が含まれます。
certs/	– 使用中の証明書のファイル
<opt_dir>/	Dr.Web for UNIX Internet Gatewaysのメインディレクトリ。次が含まれます。
bin/	– すべての製品コンポーネントの実行ファイル(Dr.Web Virus-Finding Engineを除く)
include/	– 使用中のライブラリのヘッダーファイル
lib/	– 使用中のライブラリ
man/	– システムヘルプファイル：man



ディレクトリ	コンテンツ
share/	- 以下を含む補助製品ファイル
doc/	▫ 製品ドキュメント (readmeファイル、使用許諾契約、パッケージがすでにインストールされている場合は管理者ガイド)
drweb-bases/	▫ Dr.Webのウイルスデータベースのファイル (インストール中に提供されたソースファイル)
scripts/	▫ 補助スクリプトファイル
<var_dir>/	以下を含む補助ファイルと一時ファイル:
bases/	- Dr.Webウイルスデータベースのファイル (更新バージョン)
cache/	- 更新のキャッシュ
drl/	- 使用中の更新サーバーのリスト
dws/	- Webリソースカテゴリーのデータベースのファイル
lib/	- ダイナミックリンクライブラリとしてのDr.Web Virus-Finding Engineスキャンエンジン (drweb32.dll) と、集中管理モードで作業するための設定
update/	- ダウンロード中に更新を一時的に保存するためのディレクトリ

ディレクトリで使用される表記規則の詳細については、[はじめに](#)を参照してください。

コンポーネントのカスタムインストールとアンインストール

このセクションの内容

- [カスタムインストール用の一般的なコンポーネントキット](#)
- Dr.Web for UNIX Internet Gatewaysコンポーネントのインストールとアンインストール:
 - [リポジトリからインストールする](#)
 - [ユニバーサルパッケージからインストールする](#)

必要に応じて、該当するそれぞれの[パッケージ](#)をインストール／アンインストールすることで、特定のDr.Web for UNIX Internet Gatewaysコンポーネントのみをインストール／アンインストールできます。カスタムコンポーネントのインストールまたはアンインストールは、製品のインストールと同じ方法で実行します。

コンポーネントを再インストールするには、まず初めにそのコンポーネントをアンインストールし、その後再度インストールしてください。

カスタムインストール用の一般的なコンポーネントキット


[リポジトリ](#)または[ユニバーサルパッケージ](#)からルートメタパッケージをインストールする代わりに、機能を制限してDr.Web for UNIX Internet Gatewaysをインストールする必要がある場合は、必要な機能を提供するコンポーネントパッケージのみをインストールできます。依存関係を解決するために必要なパッケージは自動的にインストールされます。以下の表は、一般的なDr.Web for UNIX Internet Gatewaysタスクを解決するために設



計されたコンポーネントセットを示しています。インストールするパッケージ列には、特定のコンポーネントスイートを取得するためにインストールする必要があるパッケージのリストがあります。

カスタムコンポーネントキット	インストールするパッケージ	インストールされるコンポーネント
コンソールスキャンのための最小キット	<ul style="list-style-type: none"> • drweb-filecheck • drweb-se 	<ul style="list-style-type: none"> • Dr.Web ConfigD • Dr.Web Ctl • Dr.Web File Checker • Dr.Web Scanning Engine • Dr.Web Updater • ウイルスデータベース
ClamAVのエミュレーションのためのスイート (clamd)	<ul style="list-style-type: none"> • drweb-clamd • drweb-se 	<ul style="list-style-type: none"> • Dr.Web ClamD • Dr.Web ConfigD • Dr.Web Ctl • Dr.Web File Checker • Dr.Web Network Checker • Dr.Web Scanning Engine • Dr.Web Updater • ウイルスデータベース
ICAPプロトコル経由でのプロキシサーバーを使用したWebサイトへのアクセスをチェックするためのスイート (アンチウイルストラフィックスキャンなし)	<ul style="list-style-type: none"> • drweb-icapd 	<ul style="list-style-type: none"> • Dr.Web ConfigD • Dr.Web Ctl • Dr.Web ICAPD • Dr.Web Updater • Dr.Web URL Checker • Webリソースカテゴリのデータベース
ICAPプロトコル経由でのプロキシサーバーを使用したWebサイトへのアクセスをチェックするためのスイート (アンチウイルストラフィックスキャンあり)	<ul style="list-style-type: none"> • drweb-icapd • drweb-netcheck • drweb-se 	<ul style="list-style-type: none"> • Dr.Web ConfigD • Dr.Web Ctl • Dr.Web ICAPD • Dr.Web Network Checker • Dr.Web Scanning Engine* • Dr.Web Updater • Dr.Web URL Checker • Webリソース、カテゴリのデータベース • ウイルスデータベース*
<div style="background-color: #e0f2f1; padding: 10px; border: 1px solid #ccc;">  <p>Dr.Web Network Checkerを介してスキャン用のデータを受信する別のサーバーでアンチウイルススキャンが実行される場合、drweb-seパッケージのインストールがスキップされる可能性があります。</p> </div>		
HTTP接続のローカルスキャンのためのスイート	<ul style="list-style-type: none"> • drweb-dws • drweb-gated • drweb-firewall 	<ul style="list-style-type: none"> • Dr.Web ConfigD • Dr.Web Ctl • Dr.Web Firewall for Linux



カスタムコンポーネントキット	インストールするパッケージ	インストールされるコンポーネント
 <p>接続のアンチウイルススキャンが必要ない場合は、drweb-netcheckおよびdrweb-seパッケージをインストールする必要はありません。Dr.Web Network Checkerを介してスキャン用のデータを受信する別のサーバーでアンチウイルススキャンが実行される場合、drweb-seパッケージのインストールがスキップされる可能性があります。望ましくないWebリソースのカテゴリにURLが該当するかをチェックする必要がない場合は、drweb-dwsパッケージのインストールがスキップされる可能性があります。</p>	<ul style="list-style-type: none">• drweb-netcheck• drweb-se	<ul style="list-style-type: none">• Dr.Web Network Checker• Dr.Web Scanning Engine*• Dr.Web Updater***• Dr.Web URL Checker• SpIDer Gate• Webリソースカテゴリのデータベース**• ウイルスデータベース*• スпамフィルター****

* drweb-seパッケージがインストールされていない場合、このコンポーネントはインストールされません。
** drweb-dwsパッケージがインストールされていない場合、このコンポーネントはインストールされません。
*** Dr.Web Updaterコンポーネントは、ウイルスデータベース、Webリソースカテゴリデータベース、およびスパムフィルターがインストールされている場合にのみインストールされます。

リポジトリからインストールされたDr.Web for UNIX Internet Gatewaysコンポーネントのインストールとアンインストール

Dr.Web for UNIX Internet Gatewaysをリポジトリからインストールした場合、コンポーネントのカスタムインストール／アンインストールには、お使いのOSで使用されているパッケージマネージャーの各コマンドを使用します。以下はその例です。

1. CentOS上にインストールされているDr.Web for UNIX Internet GatewaysからDr.Web ClamD (drweb-clamdパッケージ)をアンインストールするには、次のコマンドを使用します。

```
# yum remove drweb-clamd
```

2. Ubuntu OSにインストールされているDr.Web for UNIX Internet GatewaysにDr.Web ClamD (drweb-clamdパッケージ)を追加でインストールするには、次のコマンドを使用します。

```
# apt-get install drweb-clamd
```



必要に応じて、お使いのOSで使用されているパッケージマネージャーのヘルプを参照してください。

ユニバーサルパッケージからインストールされたDr.Web for UNIX Internet Gatewaysコンポーネントのインストールとアンインストール

Dr.Web for UNIX Internet Gatewaysがユニバーサルパッケージからインストールされていて、コンポーネントのパッケージを追加でインストールまたは再インストールする場合、Dr.Web for UNIX Internet Gatewaysのインストール元のインストールファイル(.run拡張子の付いたファイル)が必要です。このファイルを保存していない場合は、Doctor Web公式サイトからダウンロードしてください。

インストールファイルを解凍する

.runファイルを実行する際は、以下のコマンドラインパラメータを指定することもできます。

--noexec - インストールプロセスを開始せずに、Dr.Web for UNIX Internet Gatewaysのインストールファイルを解凍します。ファイルはTMPDIR環境変数で指定されたディレクトリに置かれます(通常は/tmp)。

--keep - インストール完了後にDr.Web for UNIX Internet Gatewaysのインストールファイルとインストールログを自動的に削除しません。

--target <directory> - Dr.Web for UNIX Internet Gatewaysのインストールファイルを、指定されたディレクトリ<directory>に解凍します。

.runファイルの起動時に指定できるコマンドラインパラメータの一覧を表示するには、以下のコマンドを入力します。

```
$ ./ <file_name>.run --help
```

カスタムインストールでは、解凍されたインストールファイルを使う必要があります。それらのファイルが含まれたディレクトリがない場合は、最初に以下のコマンドを入力してインストールファイルを解凍します。

```
$ ./ <file_name>.run --noexec --target <directory>
```

コマンドが実行された後、ディレクトリ<directory>内に、ネストされたディレクトリの名前<file_name>が現れます。

コンポーネントのカスタムインストール

RUNインストールファイルには、Dr.Web for UNIX Internet Gatewaysのすべてのコンポーネントのパッケージ(RPMフォーマットで)とサポートファイルが含まれています。各コンポーネントのパッケージファイルは以下の構造を持っています。

```
<component_name>_<version>~linux_<platform>.rpm
```

<version>は製品リリースのバージョンと時間が含まれたストリングで、<platform>はDr.Web for UNIX Internet Gatewaysが対象としているプラットフォームです。Dr.Web for UNIX Internet Gatewaysのコンポーネントが含まれているパッケージの名前はすべて「drweb」プレフィックスで始まります。



パッケージマネージャーはインストールキットでのパッケージのインストール時に有効になります。カスタムインストールでは、サービススクリプトinstallpkg.shを使用する必要があります。その際、まずインストールパッケージのコンテンツをディレクトリに解凍する必要があります。



パッケージをインストールするには、スーパーユーザー権限（rootユーザーの権限）が必要です。権限を昇格するには、suコマンドを使用してカレントユーザーを変更するか、またはsudoコマンドを使用して、指定されたコマンドを別のユーザーの権限で実行します。

コンポーネントパッケージのインストールまたは再インストールを開始するには、解凍したインストールキットのあるディレクトリに移動し、コンソールから（またはグラフィカルモードのターミナルであるコンソールエミュレーターから）以下のコマンドを実行します。

```
# ./scripts/installpkg.sh <package_name>
```

例:

```
# ./scripts/installpkg.sh drweb-clamd
```

Dr.Web for UNIX Internet Gateways全体のインストールを開始する必要がある場合は、以下のコマンドを使用して自動インストールスクリプトを実行します。

```
$ ./install.sh
```

その他、製品のルートメタパッケージを実行することで、すべてのDr.Web for UNIX Internet Gatewaysパッケージをインストールできます（不足しているか、誤って削除してしまったコンポーネントをインストールするため）。

```
# ./scripts/installpkg.sh drweb-internet-gateways
```

コンポーネントのカスタムアンインストール

お使いのOSがRPMフォーマットのパッケージを使用している場合、コンポーネントのカスタムアンインストールでは、OSのパッケージマネージャーの該当するアンインストールコマンドを使用します。

- Red Hat Enterprise LinuxとCentOSではyum remove <package_name>コマンドを使用します。
- Fedoraではyum remove <package_name>またはdnf remove <package_name>コマンドを使用します。
- SUSE Linuxではzypper remove <package_name>コマンドを使用します。
- MageiaとOpenMandriva Lxではurpme <package_name>コマンドを使用します。
- Alt LinuxとPCLinuxOSではapt-get remove <package_name>コマンドを使用します。

例（Red Hat Enterprise Linuxの場合）:

```
# yum remove drweb-clamd
```



お使いのOSがDEBパッケージを使用している場合 (MSVS 3.0 OSの場合も)、またはOSにパッケージマネージャーがない場合 (FreeBSD)、カスタムアンインストールでは、Dr.Web for UNIX Internet Gatewaysのインストール中に自動的にインストールされるパッケージマネージャーzypperを使用する必要があります。これを行うには、`<opt_dir>/bin` (GNU/Linuxの場合は `/opt/drweb.com/bin`) ディレクトリに移動して、以下のコマンドを実行します。

```
# ./zypper remove <package_name>
```

例:

```
# ./zypper remove drweb-clamd
```

Dr.Web for UNIX Internet Gatewaysをアンインストールする必要がある場合は、以下のコマンドを入力して[自動削除](#)スクリプトを実行します。

```
# ./uninst.sh
```

コンポーネントを再インストールするには、まずそのコンポーネントをアンインストールし、その後、インストールキットからのカスタムインストールまたはフルインストールを実行することで再度インストールします。

セキュリティサブシステムを設定する

OSに強化セキュリティサブシステムSELinuxが実装されている場合や、PARSECなどの強制アクセス制御システム (UNIXで使用されていた従来の任意モデルではないもの) が使用されている場合は、それらがデフォルト設定になっているとDr.Web for UNIX Internet Gatewaysの動作に問題が生じます。そのような場合にDr.Web for UNIX Internet Gatewaysを正常に動作させるためには、セキュリティサブシステムやDr.Web for UNIX Internet Gatewaysの設定を変更する必要があります。

[SELinuxのセキュリティポリシーの設定](#)に関する以下の詳細を参照してください。

SELinuxのセキュリティポリシーを設定する

GNU/LinuxディストリビューションにSELinux (*Security-Enhanced Linux*) が含まれている場合は、インストール後にDr.Web for UNIX Internet Gatewaysのサービスコンポーネント ([スキャンエンジン](#)など) を正常に動作させるために、SELinuxのセキュリティポリシーを設定することが必要になる場合があります。

ユニバーサルパッケージを使用したインストールの問題

SELinuxが有効になっている場合、Dr.Web for UNIX Internet Gatewaysコンポーネントを動作させる `drweb` ユーザーの作成がブロックされることがあり、[インストールファイル](#) (`.run`) からのインストールに失敗する場合があります。

`drweb` ユーザーを作成できないために、このファイルからのDr.Web for UNIX Internet Gatewaysのインストールに失敗する場合は、`getenforce` コマンドを使用してSELinuxの動作モードを確認してください。このコマンドは現在のスキャンモードを出力します。

- `Permissive` - 保護は有効ですが、許可方式が使用されています。セキュリティポリシーに違反するアクションは拒否されませんが、そのアクションに関する情報はログに記録されます。



- Enforced - 保護は有効で、制御方式が使用されています。セキュリティポリシーに違反するアクションはブロックされ、そのアクションに関する情報はログに記録されます。
- Disabled - SELinuxはインストールされていますが、有効になっていません。

SELinuxが *Enforced* モードで動作している場合は、*Permissive* モードに変更してください。それには、以下のコマンドを使用します。

```
# setenforce 0
```

このコマンドはSELinuxの *Permissive* モードを一時的に(次の再起動まで)有効にします。



setenforceコマンドで有効にした動作モードに関係なく、OSの再起動後、SELinuxは設定で指定された安全な動作モードに戻ります (SELinuxの設定ファイルは通常、`/etc/selinux` ディレクトリにあります)。

Dr.Web for UNIX Internet Gatewaysが正常にインストールされた後、製品を起動させる前に *Enforced* モードを再度有効にしてください。それには、以下のコマンドを使用します。

```
# setenforce 1
```

Dr.Web for UNIX Internet Gatewaysの動作に関する問題

SELinuxの実行中にいくつかのDr.Web for UNIX Internet Gatewaysコンポーネント (`drweb-se` や `drweb-filecheck` など) が起動できないことがあります。これにより、オブジェクトのスキャンやファイルシステムのモニタリングができなくなります。これらのコンポーネントが起動できない場合は、`syslog` サービスによって管理されるシステムログ (通常このログは `/var/log/` ディレクトリにあります) に [119](#) および [120](#) のエラーメッセージが表示されます。

SELinuxセキュリティシステムによってアクセスが拒否された場合、そのようなイベントのログが記録されます。一般的に、システムでauditデーモンが使用されている場合、audit (監査) に関するログが `/var/log/audit/audit.log` ファイルに保存されます。それ以外の場合、ブロックされた動作に関するメッセージが一般的なログファイル (`/var/log/messages` または `/var/log/syslog`) に保存されません。

SELinuxにブロックされているために製品のスキャンコンポーネントが機能しない場合は、該当するコンポーネントに対して特別な *セキュリティポリシー* を設定する必要があります。



一部のGNU/Linuxディストリビューションには、以下のユーティリティが備わっていません。その場合、ユーティリティの追加パッケージをインストールする必要がある場合があります。

SELinuxのセキュリティポリシーを設定する

1. SELinuxのポリシーソースコードを記述したファイル (`.te` ファイル) を新たに作成します。このファイルでは、記述されているポリシーモジュールに関連した制限を規定します。このポリシーソースコードは以下のいずれかの方法で作成できます。



- 1) `audit2allow`ユーティリティの使用は、最もシンプルな方法です。ユーティリティはシステムログファイル内のアクセス拒否に関するメッセージから`permissive`ルールを生成します。自動でメッセージを検索するよう設定するか、手動でログファイルへのパスを指定できます。



この方法は、Dr.Web for UNIX Internet GatewaysのコンポーネントがSELinuxのセキュリティポリシーに違反していて、それらのイベントが監査ログファイルに記録されている場合にのみ使用できます。そうでない場合、そのようなイベントが起こるのを待つか、`policygentool`ユーティリティを使用して強制的に`permissive`ポリシーを作成してください(下記参照)。

`audit2allow`ユーティリティは、`policycoreutils-python`パッケージまたは`policycoreutils-devel`パッケージ(Red Hat Enterprise Linuxの場合はCentOS、Fedora OSの場合はバージョンにより異なる)にあり、DebianおよびUbuntu OSの場合は`python-sepolgen`パッケージにあります。

`audit2allow`の使用例:

```
# grep drweb-se.real /var/log/audit/audit.log | audit2allow -M drweb-se
```

この例では、`drweb-se`コンポーネントに対するアクセス拒否メッセージを見つけるために、`audit2allow`ユーティリティが`/var/log/audit/audit.log`ファイル内で検索を実行します。

作成されるファイルは、ポリシーソースファイル`drweb-se.te`と、インストール可能な`drweb-se.pp`ポリシーモジュールの2つです。

システム監査ログ内でセキュリティ違反イベントが見つからなかった場合、ユーティリティはエラーメッセージを返します。

ほとんどの場合、`audit2allow`ユーティリティで作成したポリシーファイルを変更する必要はありません。したがって、[手順4](#)の`drweb-se.pp`ポリシーモジュールのインストールに進むことを推奨します。



`audit2allow`ユーティリティは`semodule`コマンドの呼び出しを出力します。この出力をコマンドラインにコピーして実行すると、[手順4](#)が完了します。Dr.Web for UNIX Internet Gatewaysコンポーネント用に自動的に生成されたセキュリティポリシーを変更する場合にのみ、[手順2](#)に進みます。

- 2) `policygentool`ユーティリティを使用する。そのためには、異なる方法で処理するコンポーネントの名前とその実行ファイルへのフルパスを指定します。



Red Hat Enterprise LinuxとCentOS向けの`selinux-policy`パッケージに含まれている`policygentool`ユーティリティは正常に機能しない場合があります。その場合は`audit2allow`ユーティリティを使用してください。

`policygentool`を使用したポリシー作成の例:

- `drweb-se`コンポーネントの場合:

```
# policygentool drweb-se /opt/drweb.com/bin/drweb-se.real
```

- `drweb-filecheck`コンポーネントの場合:

```
# policygentool drweb-filecheck /opt/drweb.com/bin/drweb-filecheck.real
```




ドメインを作成するための一般的なプロパティをいくつか指定するように求められます。その後、ポリシーを決定する以下の3つのファイルが(コンポーネントごとに)作成されます。

`<module_name>.te`、`<module_name>.fc`、`<module_name>.if`

2. 必要に応じて、生成されたポリシーソースファイル`<module_name>.te`を編集し、その後、`checkmodule`ユーティリティを使用して、ローカルポリシーのこのソースファイルをバイナリ形式に変換(`.mod`ファイル)します。



コマンドを正常に実行するには、システムに`checkpolicy`パッケージがインストールされている必要があります。

使用例:

```
# checkmodule -M -m -o drweb-se.mod drweb-se.te
```

3. `semodule_package`ユーティリティを使用して、インストール用のポリシーモジュールを作成します(`.pp`ファイル)。

例:

```
# semodule_package -o drweb-se.pp -m drweb-se.mod
```

4. 作成されたポリシーモジュールをインストールするには、`semodule`ユーティリティを使用します。

例:

```
# semodule -i drweb-se.pp
```

SELinuxの動作と設定に関する詳細は、お使いのUNIXディストリビューションのマニュアルを参照してください。



開始する

1. インストールされたDr.Web for UNIX Internet Gatewaysの使用を開始するために、[キーファイル](#)を入手してインストールした上で[有効化](#)する必要があります。
2. Dr.Web for UNIX Internet Gatewaysの[動作確認のために](#)さらにスキャンすることをお勧めします。
3. Dr.Web for UNIX Internet Gatewaysを、使用しているHTTPプロキシサーバーと統合します（提供されているSquidプロキシサーバーとの統合に関する[説明](#)を参照してください）。
4. ローカルWebサーバーを外部ネットワークの脅威から保護するために、SpIDer Gateモニターの設定を[変更](#)します。
5. 外部のプロキシサーバーを使用していない場合は、SpIDer Gateのプロキシモードを[設定](#)します。
6. どのコンポーネントが実行されているかを確認し、サーバーの保護に必要な場合には、デフォルトで無効になっているコンポーネントを追加で有効にします（ディストリビューションによって異なりますが、[Dr.Web ClamD](#)または[Dr.Web SNMPD](#)コンポーネントなど）。



追加コンポーネントを有効にすること以外に、デフォルトの設定を調整するなど、他のアクションを実行する必要がある場合があります。

インストール済みおよび実行中のコンポーネントとその設定のリストを表示するには、次のいずれかを使用します。

- [コマンドラインベース管理ツール](#)のDr.Web Ctl。drweb-ctl appinfo、drweb-ctl cfshow、およびdrweb-ctl cfsetコマンドを使用します。
- Dr.Web for UNIX Internet Gatewaysの管理用[ウェブインターフェース](#)（初期設定では、ウェブブラウザから<https://127.0.0.1:4443/>にアクセスすると利用できます）。

製品の登録と有効化

このセクションの内容

- [ライセンスを購入・登録する](#)
- [デモライセンスを取得する](#)
- [キーファイルのインストール](#)
- [2回目以降の登録](#)

ライセンスを購入・登録する

ライセンスを購入すると、製品コンポーネントとウイルスデータベースの更新がDoctor Web更新サーバーから定期的にダウンロードされます。さらに、購入した製品をインストールまたは使用するときに問題が発生した場合は、Doctor Webまたはそのパートナーが提供するテクニカルサポートサービスを利用できます。

Dr.Web製品の購入や製品のシリアル番号の入手は、[パートナー](#)または[オンラインストア](#)から可能です。ライセンスオプションの詳細については、Doctor Web公式Webサイト（https://license.drweb.com/license_manager）にアクセスしてください。

ライセンス登録は、ユーザーがDr.Web for UNIX Internet Gatewaysの正規ユーザーであることを証明し、ウイルスデータベースの定期的な更新を含むアンチウイルスの機能を有効にするために必要です。インストールが



完了したら、製品を登録してライセンスを有効化することを推奨します。購入したライセンスは、Doctor Webの公式Webサイト (<https://products.drweb.com/register/v4>) で有効化できます。

有効化の際には、購入したライセンスのシリアル番号を入力する必要があります。シリアル番号はDr.Web for UNIX Internet Gatewaysと一緒に提供されるか、オンラインでライセンスを購入または更新した際にメールで提供されます。

デモライセンスを取得する

ご利用のDr.Web for UNIX Internet Gatewaysの試用期間は、Doctor Webの公式Webサイト (<https://download.drweb.com/demoreq/biz/v2>) で確認できます。製品を選択して登録フォームに記入すると、Dr.Web for UNIX Internet Gatewaysを有効化するためのシリアル番号またはキーファイルが記載されたメールが届きます。



同じコンピューターでの2回目以降の試用期間は、一定の期間が経過した後に利用できません。

Dr.Web Ctl(`drweb-ctl`) コマンドラインツールの**ライセンスコマンド**を使用すると、登録されたライセンスのシリアル番号のデモキーファイルまたはライセンスされたキーファイルを自動的に取得できます。

キーファイルのインストール

キーファイルは、Dr.Web for UNIX Internet Gatewaysの購入したライセンスまたは有効化した試用期間に対応する、ローカルコンピューター上に保存される特別なファイルです。このファイルには提供されたライセンスまたは試用期間に関する情報が含まれ、また、このファイルに応じて使用権限が規定されます。



Dr.Web for UNIX Internet Gatewaysの動作中、キーファイルはデフォルトの `<etc_dir>` ディレクトリ (GNU/Linuxの場合は `/etc/opt/drweb.com`) に `drweb32.key` という名前 で置かれている必要があります。

Dr.Web for UNIX Internet Gatewaysのコンポーネントは、キーファイルが使用可能かつ有効であるかどうかを定期的に確認します。編集されることを防ぐため、キーファイルはデジタル署名されています。キーファイルを編集すると無効になります。誤って無効にしてしまうことを防ぐため、キーファイルをテキストエディターで開かないことをお勧めします。

有効なキーファイル (正規またはデモライセンス) が見つからない場合、またはライセンスの有効期限が切れている場合、有効なキーファイルがインストールされるまでアンチウイルスコンポーネントの動作はブロックされます。

ライセンスキーファイルは有効期限が切れるまで保管しておき、Dr.Web for UNIX Internet Gatewaysの再インストールや、別のコンピューターへのインストールにはそのライセンスキーファイルを使用することを推奨します。この場合、登録時に指定したのと同じ製品シリアル番号と顧客データを使用する必要があります。



メールメッセージでは、Dr.Webキーファイルは通常、zipアーカイブに圧縮されて転送されます。Dr.Web for UNIX Internet Gatewaysのアクティベーション用のキーファイルを含むアーカイブは、通常はdrweb32.zipまたはagent.zipという名前です。メッセージに複数のアーカイブが含まれている場合は、agent.zipアーカイブを使用する必要があります。

キーファイルをインストールする前に、アーカイブを適宜解凍し、そこからキーファイルを抽出して、使用可能な任意のディレクトリ(たとえば、ホームディレクトリやUSBフラッシュドライブ)に保存してください。

製品の有効なライセンスに対応するキーファイルをお持ちの場合(キーファイルをメールで受け取った場合、またはDr.Web for UNIX Internet Gatewaysを別のサーバー上で使用する場合など)、そのキーファイルへのパスを指定することでDr.Web for UNIX Internet Gatewaysを有効化できます。その場合は、次の操作を行います。

1. アーカイブの場合はキーファイルを解凍します。
2. 次のいずれかを実行してください:
 - キーファイルを<etc_dir>ディレクトリにコピーし、必要に応じてファイル名をdrweb32.keyに変更します。
 - Dr.Web for UNIX Internet Gateways設定ファイルで、KeyPathパラメータ値にキーファイルパスを指定します。
3. 次のコマンドを入力して、Dr.Web for UNIX Internet Gatewaysの設定をリロードします。

```
# drweb-ctl reload
```

すべての変更が適用されます。

また、次のコマンドを使用することもできます。

```
# drweb-ctl cfset Root.KeyPath <path to the key file>
```

この場合、Dr.Web for UNIX Internet Gatewaysの再起動は不要です。キーファイルは<etc_dir>ディレクトリにコピーされず、元の場所に残ります。



<opt_dir>、<etc_dir>、<var_dir>の表記規則の詳細は、はじめにを参照してください。

キーファイルが<etc_dir>ディレクトリにコピーされない場合は、ユーザーはファイルが破損や削除から保護されていることを確認する必要があります。キーファイルがシステムから誤って削除される可能性があるため、この方法は推奨されません(たとえば、キーファイルが存在するディレクトリが定期的にクリーンアップされる場合)。キーファイルを紛失した場合は、サポートを要求して新しいキーファイルを取得できますが、要求できる回数には制限があります。

2回目以降の登録

キーファイルを紛失したが、既存のライセンスの有効期限が切れていない場合は、前回の登録時に指定した個人データを入力して、再度登録する必要があります。別のメールアドレスを使用できます。この場合、ライセンスキーファイルは新しく指定されたアドレスに送信されます。



キーファイルのリクエスト回数には制限があります。その数を超えてリクエストが送信された場合、キーファイルは配信されません。紛失したキーファイル入手するには、Doctor Web [テクニカルサポート](#) に連絡して問題の詳細を説明し、シリアル番号の登録時に入力した個人データを伝えてください。ライセンスキーファイルはメールで送信されます。

キーファイルがメールで送信されたら、手動で [インストール](#) する必要があります。

製品の動作確認

EICAR (European Institute for Computer Anti-Virus Research) テストを行うと、ウイルスをシグネチャで検出するアンチウイルスプログラムの動作を確認できます。このテストは、新しくインストールしたアンチウイルスツールのウイルス検出の動作を、コンピューターを危険にさらすことなくテストできるように特別に設計されています。

EICAR は実際にはウイルスではありませんが、多くのアンチウイルスプログラムによってウイルスとして処理されるようにできています。この「ウイルス」を検出すると、Dr. Web のアンチウイルス製品は「EICAR Test File (NOT a Virus!)」という表示を出します。その他のアンチウイルスツールも同じようにユーザーに警告します。EICAR テストファイルは MS DOS/MS Windows 向けの 68 バイトの COM ファイルで、実行すると、ターミナル画面またはコンソールエミュレーターに次のラインを出力します。

```
EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
```

EICAR テストファイルは、次の文字列のみを含んでいます。

```
X50!P%0AP[4\pZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

上記の文字列でファイルを作成すると、「ウイルス」として認識されるテストファイルができあがります。

Dr. Web for UNIX Internet Gateways が正常に動作していれば、テストファイルはスキャンの種類に関係なくファイルシステムのスキャン中に検出され、検出された脅威について「EICAR Test File (NOT a Virus!)」と通知されます。

EICAR テストを使用した Dr. Web for UNIX Internet Gateways の動作の確認を、コマンドラインから実行する場合のコマンドの例:

```
$ tail <opt_dir>/share/doc/drweb-se/readme.eicar | grep X50 > testfile &&  
drweb-ctl rawscan testfile && rm testfile
```

このコマンドは、`<opt_dir>/share/doc/drweb-se/readme.eicar` ファイル (Dr. Web for UNIX Internet Gateways に付属) から EICAR テストファイルの本文を表す文字列を抽出し、それを現在のディレクトリに作成された `testfile` という名前のファイルに書き込みます。その後、このファイルのスキャンしてから削除します。



上記のテストを行うには、カレントディレクトリへの書き込みアクセスが必要です。また、ディレクトリに `testfile` という名前のファイルが含まれていないことを確認してください (必要に応じて、コマンド内でファイル名を変更してください)。

`<opt_dir>`、`<etc_dir>`、`<var_dir>` の表記規則の詳細は、[はじめに](#) を参照してください。



テストウイルスが検出されると、以下のメッセージが表示されます。

```
<path to the current directory>/testfile - infected with EICAR Test File (NOT a Virus!)
```

テスト中にエラーが発生した場合は、既知のエラーの説明を参照してください([付録F. 既知のエラー](#)を参照)。

受信HTTPトラフィックにウイルスが含まれているかどうかをテストするには:

Webブラウザ経由

1. ブラウザを開き、プロキシサーバー設定に移動します。
2. ICAPの適切なプロキシサーバー設定を入力します。
3. Webページ<https://www.eicar.org/download/eicar.com>にアクセスします。ファイルが感染しているという通知がブラウザウィンドウに表示されます。

コンソール経由

次のリクエストを行います。

```
curl -x 127.0.0.1:3128 https://www.eicar.org/download/eicar.com
```

リクエストしたファイルが感染しているという通知がレスポンスに表示されます。

Squidプロキシサーバーとの統合

このセクションの内容

- [Dr.Web ICAPDを設定する](#)
- [Squidを設定する](#)
- [Squidのアドバンス設定](#)

Dr.Web ICAPDを設定する

Dr.Web ICAPDとSquid HTTPプロキシサーバーを統合するには、Dr.Web ICAPDの[設定セクション](#) ([ICAP] セクション)で現在のパラメータ値を確認し、必要に応じて変更する必要があります。

- ListenAddressパラメータに、HTTPプロキシサーバーからの接続を待機するDr.Web ICAPDによってリスンされるネットワークソケットのアドレス(<IP address>:<port>)を指定します(デフォルトでは127.0.0.1:1344ソケットを使用します)。
- Block*設定で、Dr.Web ICAPDがブロックまたは許可するWebサイトのカテゴリと脅威の種類を有効または無効にします。
- 必要に応じて、BlackListパラメータの値として、ブロックするWebサイトのリストを指定します。WhiteListパラメータの値には、ブロックしてはいけないWebサイトのリストを指定できます。



BlackListパラメータはWhiteListよりも優先されます。両方のパラメータのリストにドメインが含まれている場合、そのドメインはブロックされます。



- Webサイトへのアクセスをより詳細な方法で(さまざまな条件に基づいて)設定するには、[スキャンルール](#)を編集します。



設定のDr.Web ICAPDのセクションにあるUsePreview、Use204、AllowEarlyResponseパラメータのデフォルト値を使用すると、Internet Content Adaptation Protocol (ICAP) の該当する機能をコンポーネントで使用できます(つまり、ICAPプレビューモードを使用する、ICAPプレビューモード以外でも204ステータスコードを返す、リクエスト全体がプロキシサーバーから受信される前に「初期」レスポンスの送信を開始するといった操作が可能になります)。HTTPリクエスト処理に問題がない場合は、デフォルト値を変更しないことをお勧めします。

すべての設定を調整したら、Dr.Web for UNIX Internet Gatewaysを次の[コマンド](#)で再起動します。

```
# drweb-ctl reload
```

設定デーモンDr.Web ConfigDは、次のコマンドでも再起動できます。

```
# service drweb-configd restart
```

Squidを設定する

SquidとDr.Web ICAPD間のインタラクションを有効にするには、`squid.conf`設定ファイル(通常は`/etc/squid3/`にあります)を編集してICAPの使用を許可します。Squidを設定するには、以下の手順に従ってください。

1. Squidの設定でICAPを有効にします。
2. SquidのICAPサービスとしてDr.Web ICAPDを登録します。
3. *ICAPプレビューモード*を有効にします(オプション)。
4. Dr.Web ICAPDのルール内で使用できるように、クライアントのデータ(プロキシサーバーでの認証にパスしたユーザーのIPアドレスとユーザー名)の送信を許可します(オプション)。
5. Dr.Web ICAPDとSquid間の持続的接続のサポートを有効にします(オプション。持続的接続を有効にする必要はありませんが、Dr.Web ICAPDと連携するSquidのパフォーマンスを高めることができます)。



- SquidでICAP経由のHTTP要求 (*REQMOD*)とHTTP応答 (*RESPMOD*)をチェックするには、該当する種類の2つのICAPサービスを追加します。
- SquidでDr.Web ICAPDをICAPサービスとして使用するには、`icap_service`で指定したアドレスとポートが、Dr.Web ICAPDの設定のListenAddressパラメータで指定したアドレスとポートと一致する必要があります。
- `icap_preview_size`パラメータの値が0ではない場合、Dr.Web ICAPDはSquidでは機能しません。
- クライアントのIPアドレスとユーザー名は、ICAPリクエストのX-Client-UsernameおよびX-Client-IPヘッダーでSquidによってDr.Web ICAPDに送られます。これらのヘッダーの値は、Squidでデフォルトで使用される方法によってエンコードされている必要があります。エンコード方法に影響を与えるSquidの設定(`icap_client_username_encode`および`icap_client_username_header`ヘッダー)は変更しないでください。



SquidがICAPのサポート付きで構築されている(すなわち、`--enable-icap-client`オプションを指定してコンパイルされている)必要があります。そうでない場合、SquidとDr.Web ICAPD間の接続は確立できません。



HTTPSプロトコルを使用するには、SquidがSSLサポート付きでビルドされている(すなわち、`--with-openssl`および`--enable-ssl-crttd`オプションでコンパイルされている)必要があります。Squidの設定でSSLバンピングを有効にする必要があります。

設定できるパラメータのリストは、使用しているSquidサーバーのバージョンによって異なります(Squidバージョン3.2(およびそれ以降)、3.1、3.0の設定については、後述の説明を参照)。

ここに示す例に従って、Squidの設定ファイルを変更します。

例に示されているパラメータがすでにコメントアウトされている場合は、コメントを外します。必要なパラメータがない場合は、それらのパラメータをSquidの設定ファイルに追加します。



Dr.Web ICAPDとSquid間のインタラクションを設定する場合は、#1と#2の手順のみが必須です。以下に示すその他の設定のうち、不要な設定はSquid設定ファイルに追加しないでください。

Squid 3.2以降のバージョンの場合

```
#1
icap_enable on

#2
icap_service i_req reqmod_precache bypass=0 icap://127.0.0.1:1344/reqmod
icap_service i_res respmod_precache bypass=0 icap://127.0.0.1:1344/respmod

adaptation_access i_req allow all
adaptation_access i_res allow all

#3
icap_preview_enable on
icap_preview_size 0

#4 (In Squid 3.2, the icap_send_client_ip and icap_send_client_username
parameters have been renamed)
adaptation_send_client_ip on
adaptation_send_username on

#5
icap_persistent_connections on
```

Squid 3.1の場合

```
#1
icap_enable on

#2 (In Squid 3.1, the format used to configure a service has been changed
```



```
and the icap_access parameter has been renamed)
icap_service i_req reqmod_precache bypass=0 icap://127.0.0.1:1344/reqmod
icap_service i_res respmod_precache bypass=0 icap://127.0.0.1:1344/respmod

adaptation_access i_req allow all
adaptation_access i_res allow all

#3
icap_preview_enable on
icap_preview_size 0

#4
icap_send_client_ip on
icap_send_client_username on

#5
icap_persistent_connections on
```

Squid 3.0の場合

```
#1
icap_enable on

#2
icap_service i_req reqmod_precache 0 icap://127.0.0.1:1344/reqmod
icap_service i_res respmod_precache 0 icap://127.0.0.1:1344/respmod

icap_class icapd_class_req i_req
icap_class icapd_class_resp i_res

icap_access icapd_class_req allow all
icap_access icapd_class_resp allow all

#3
icap_preview_enable on
icap_preview_size 0

#4
icap_send_client_ip on
icap_send_client_username on

#5
icap_persistent_connections on
```

設定の変更後、Squidを再起動します。



Squidのアドバンス設定: データサイズの制限

必要に応じて、SquidがICAPプロトコル経由でスキャンのために送信するデータのサイズを制限できます。そのためには、設定ファイルでContent-Lengthヘッダーの値を指定します(バイト単位 of 特定のサイズまたは正規表現)。たとえば、次のように指定します。

```
acl <name> rep_header Content-Length ^[0-9]{7,}$
```

(サーバーレスポンスのヘッダーContent-Lengthに999999より大きい数値が含まれている場合、条件<name>は有効です)。

上記の例の条件は、ICAPプロトコルを介したサーバーレスポンスのスキャンをallow(許可)またはdeny(拒否)するために使用できます(Squidの接続パラメータでは、allの語を条件名<name>に置き換える必要があります)。次の例は、条件<name>が有効であるレスポンスのスキャンを拒否するために使用する設定を示しています。

```
#Squid 3.1 and later versions
adaptation_access i_res deny <name>

#Squid 3.0 and later versions
icap_access icapd_class_resp deny <name>
```



WebサーバーのレスポンスにContent-Lengthヘッダーがない場合があります。この場合、データサイズの制限に関する設定は適用されません。

SquidのWebトラフィックの制限の設定に関する詳細については、[公式マニュアル](#)に記載されています。



設定ファイルの編集後、変更した設定を有効にするためにSquidを再起動します。

ローカルWebサーバーを保護する

このセクションの内容

- [接続のリダイレクトを設定する](#)
- [スキャン設定](#)



このオプションはGNU/Linux OSの製品 ディストリビューションでのみ使用できます。

Dr.Web for UNIX Internet Gatewaysがインストールされているのと同じホスト上で実行されているWebサーバーを保護するには、サーバーに届くすべてのトラフィックをSpIDer Gateモニターでスキャンできるようにする必要があります。



接続のリダイレクトを設定する

Webサーバー保護を設定するには、Dr.Web Firewall for Linuxの[設定](#)（[LinuxFirewall] セクション）で、設定ファイルの複数のパラメータ値を変更します。

パラメータ	必要な値
InspectHttp	On
AutoconfigureIptables	Yes
AutoconfigureRouting	Yes
LocalDeliveryMark	Auto
ClientPacketsMark	Auto
ServerPacketsMark	Auto
TproxyListenAddress	127.0.0.1:0 Dr.Web Firewall for Linuxの操作に特別なIPアドレスまたはポートを使用する場合は、ここで指定します。
InputDivertEnable	Yes
InputDivertNfqueueNumber	Auto
InputDivertConnectTransparently	Yes

Dr.Web Firewall for Linuxの設定を表示および変更するには、次の方法を使用します。

- [コマンドラインベース管理ツールDr.Web Ctl](#)（`drweb-ctl cfshow`および`drweb-ctl cfset`コマンドを使用します）。

次は、コマンドの例です。

```
# drweb-ctl cfset LinuxFirewall.InputDivertEnable Yes
```

このコマンドを実行すると、HTTPプロトコルが使用されており、InspectHttpパラメータ値がOnに設定されている場合に、受信データがSpIDer GateによってスキャンされるようにDr.Web Firewall for Linuxが設定されます。

- Dr.Web for UNIX Internet Gatewaysの管理用[Webインターフェース](#)（デフォルトでは、Webブラウザから `https://127.0.0.1:4443/` にアクセスすると利用できます）。

HTTPSプロトコルを介して転送されたデータをスキャンするには、さらに次の手順を実行します。

- 次のコマンドを実行して対応するパラメータの値を指定することで、SSL/TLS経由で送信されるトラフィックのスキャンを有効にします。

```
# drweb-ctl cfset LinuxFirewall.UnwrapSsl Yes
```

スキャンルールが自動的に更新されるように、`drweb-ctl` ツールの `cfset` コマンドまたは管理Webインターフェースを使用することを推奨します。スキャンルールはこのパラメータに依存します。



- 次のコマンドを実行して、保護されたSSL/TLSチャネルへの統合にDr.Web for UNIX Internet Gatewaysが使用する証明書をエクスポートします。

```
$ drweb-ctl certificate > <cert_name>.pem
```

証明書をPEM形式で保存するために使用されるファイルの名前を指定する必要があります。

- 取得した証明書を信頼できる証明書のシステムリストに追加し、可能な場合には、それをWebクライアント（ブラウザ）およびWebサーバー用の信頼できる証明書として書き込みます。詳細は、[付録E. SSL証明書を生成する](#)のセクションを参照してください。

スキャン設定

設定ファイルのLinuxFirewallセクションで、次のパラメータを指定します。

1. 転送データのスキャンパラメータ(ScanTimeout、HeuristicAnalysis、PackerMaxLevel、ArchiveMaxLevel、MailMaxLevel、ContainerMaxLevel、MaxCompressionRatio)。これらのパラメータは、スキャンの長さとしリソース強度を制限します。きめ細かい設定が不要な場合は、パラメータデータの値をデフォルトの状態にしておくことを推奨します。
2. 望ましくないURLやコンテンツをブロックするためのBlock*パラメータ。
3. 受信したデータをスキャンできない場合にSpIDer Gateのアクションを指定するためのBlockUncheckedパラメータ。

フィルタリングルールの詳細な設定については、[Luaプロシージャ](#)またはRuleSet[ルール](#)を編集してください。

すべての設定を調整したら、Dr.Web for UNIX Internet Gatewaysを次の[コマンド](#)で再起動します。

```
# drweb-ctl reload
```

設定デーモンDr.Web ConfigDは、次のコマンドでも再起動できます。

```
# service drweb-configd restart
```

SpIDer Gateをプロキシモードで使用する

このセクションの内容

- [プロキシモードを設定する](#)
- [スキャン設定](#)



このオプションはGNU/Linux OSの製品 ディストリビューションでのみ使用できます。

ICAPを使用して、またはClamAVプロトコル[経由で](#)([Dr.Web ClamD](#)コンポーネントを直接使用して)Dr.Web for UNIX Internet Gatewaysと[通信](#)できるHTTPプロキシサーバーがインターネットゲートウェイにない場合は、インターネット経由で広がる脅威からローカルネットワークを保護するために、Dr.Web for UNIX Internet Gatewaysがインストールされているインターネットゲートウェイ経由で受信した情報が[SpIDer Gate](#)モニターによってスキャンされるように[Dr.Web Firewall for Linux](#)を設定します(透過プロキシモード)。



プロキシモードを設定する

透過プロキシモードを設定するには、Dr.Web Firewall for Linux(セクション[LinuxFirewall])の**設定**のセクションで、設定ファイルの一部のパラメータ値を次のように変更します。

パラメータ	必要な値
InspectHttp	On
AutoconfigureIptables	Yes
AutoconfigureRouting	Yes
LocalDeliveryMark	Auto
ClientPacketsMark	Auto
ServerPacketsMark	Auto
TproxyListenAddress	127.0.0.1:0 Dr.Web Firewall for Linuxの操作に特別なIPアドレスまたはポートを使用する場合は、ここで指定します
ForwardDivertEnable	Yes
ForwardDivertNfqueueNumber	Auto
ForwardDivertConnectTransparently	Yes

Dr.Web Firewall for Linuxの設定を表示して変更するには、次の方法を使用します。

- [コマンドラインベース管理ツールDr.Web Ctl](#)(`drweb-ctl cfshow`および`drweb-ctl cfset`コマンドを使用します)。

次は、コマンドの例です。

```
# drweb-ctl cfset LinuxFirewall.ForwardDivertEnable Yes
```

このコマンドを実行すると、HTTPプロトコルが使用されており、対応するInspectHttpパラメータ値がOnに設定されている場合に、受信データがSpIDer GateIによってスキャンされるようにDr.Web Firewall for Linuxが設定されます。

- Dr.Web for UNIX Internet Gatewaysの管理用[Webインターフェース](#)(デフォルトでは、Webブラウザから `https://127.0.0.1:4443/` にアクセスすると利用できます)。

HTTPSプロトコルを介して転送されたデータをスキャンするには、次の手順を実行します。

- SSL/TLS経由で送信されるトラフィックのスキャンを有効にします。

```
# drweb-ctl cfset LinuxFirewall.UnwrapSsl Yes
```

すべての従属パラメータの値が自動的に変更されるように、ツール`drweb-ctl`またはWebインターフェースの`cfset`コマンドを使用して、このパラメータに新しい値を適用します。



- 次のコマンドを実行して、保護されたSSL/TLSチャネルへの統合にDr.Web for UNIX Internet Gatewaysが使用する証明書をエクスポートします。

```
$ drweb-ctl certificate > <cert_name>.pem
```

証明書をPEM形式で保存するために使用されるファイルの名前を指定する必要があります。

- 信頼できる証明書のシステムリストに証明書を追加し、それをWebクライアント(ブラウザ)およびWebサーバー用の信頼できる証明書として指定します。詳細は、[付録E. SSL証明書を生成する](#)のセクションを参照してください。

スキャン設定

設定ファイルのLinuxFirewallセクションで、次のパラメータを指定します。

1. 転送データのスキャンパラメータ(ScanTimeout、HeuristicAnalysis、PackerMaxLevel、ArchiveMaxLevel、MailMaxLevel、ContainerMaxLevel、MaxCompressionRatio)。これらのパラメータは、スキャンの長さとしリソース強度を制限します。きめ細かい設定が不要な場合は、パラメータデータの値をデフォルトの状態にしておくことを推奨します。
2. 望ましくないURLやコンテンツをブロックするためのBlock*パラメータ。
3. 受信したデータをスキャンできない場合にSpIDer Gateのアクションを指定するためのBlockUncheckedパラメータ。

フィルタリングルールの詳細な設定については、[Luaプロシージャ](#)またはRuleSet[ルール](#)を編集してください。

すべての設定を調整したら、Dr.Web for UNIX Internet Gatewaysを次のコマンドで再起動します。

```
# drweb-ctl reload
```

設定デーモンDr.Web ConfigDは、次のコマンドでも再起動できます。

```
# service drweb-configd restart
```



簡単な説明

このセクションの内容

- HTTPプロキシとWebサーバーの操作：
 - [Dr.Web for UNIX Internet GatewaysをSquidに接続する方法](#)
 - [Webサーバーを保護する方法](#)
 - [SpIDer Gateのプロキシモードを設定する方法](#)
- Dr.Web for UNIX Internet Gatewaysの一般的な動作：
 - [Dr.Web for UNIX Internet Gatewaysを再起動する方法](#)
 - [集中管理サーバーに接続する方法](#)
 - [集中管理サーバーから切断する方法](#)
 - [Dr.Web for UNIX Internet Gatewaysを有効化する方法](#)
 - [Dr.Web for UNIX Internet Gatewaysをアップグレードする方法](#)
 - [Dr.Web for UNIX Internet Gatewaysコンポーネントを追加または削除する方法](#)
 - [Dr.Web for UNIX Internet Gatewaysコンポーネントの動作を管理する方法](#)
 - [Dr.Web for UNIX Internet Gatewaysのログを表示する方法](#)

Dr.Web for UNIX Internet GatewaysをSquidに接続する方法

[Squidプロキシサーバーとの統合セクション](#)の指示に従ってください。

Webサーバーを保護する方法

[ローカルWebサーバーを保護するセクション](#)の指示に従ってください。

SpIDer Gateのプロキシモードを設定する方法

[SpIDer Gateをプロキシモードで使用するセクション](#)の指示に従ってください。



Dr.Web for UNIX Internet Gatewaysを再起動する方法

Dr.Web for UNIX Internet Gatewaysがすでに実行されているときに再起動するには、Dr.Web ConfigD 設定デーモンを管理するスクリプトを使用することもできます。デーモンを起動、停止、または再起動すると、それぞれDr.Web for UNIX Internet Gatewaysが起動、停止、または再起動されます。

Dr.Web ConfigDの動作を制御するシェルスクリプトは、標準のOSディレクトリ(GNU/Linuxの場合は /etc/init.d/、FreeBSDの場合は /usr/local/etc/rc.d/)にあります。スクリプトの名前は drweb-configd です。次のパラメータがあります。

パラメータ	説明
start	実行されていない場合は、Dr.Web ConfigDを起動します。Dr.Web ConfigDが起動すると、Dr.Web ConfigDはDr.Web for UNIX Internet Gatewaysに必要なすべてのコンポーネントを起動します。
stop	実行されている場合は、Dr.Web ConfigDをシャットダウンします。Dr.Web ConfigDがシャットダウンすると、Dr.Web ConfigDはDr.Web for UNIX Internet Gatewaysのすべてのコンポーネントもシャットダウンします。
restart	Dr.Web ConfigDを再起動(シャットダウンしてから起動)します。Dr.Web ConfigDはシャットダウンしてから、Dr.Web for UNIX Internet Gatewaysのすべてのコンポーネントを起動します。Dr.Web ConfigDが実行されていない場合、このパラメータには起動と同じ効果があります。
condrestart	実行されている場合にのみ、Dr.Web ConfigDを再起動します。
reload	コンポーネントが実行されている場合は、HUPシグナルをDr.Web ConfigDに送信します。Dr.Web ConfigDはこのシグナルをDr.Web for UNIX Internet Gatewaysのすべてのコンポーネントに転送します。このパラメータは、すべてのコンポーネントに設定を再度読み込ませるために使用されます。
status	Dr.Web ConfigDの現在の状態をコンソールに出力します。

たとえば、GNU/Linux OSでDr.Web for UNIX Internet Gatewaysを再起動(実行されていない場合は起動)するには、次のコマンドを使用します。

```
# /etc/init.d/drweb-configd restart
```

集中管理サーバーに接続する方法

1. 集中管理サーバーのアドレスとその証明書のファイルをアンチウイルスネットワーク管理者から入手します。ワークステーションのIDとパスワードや、メイングループと課金プラングループのIDなど、追加パラメータが必要になる場合もあります。
2. Dr.Web for UNIX Internet Gatewaysで提供される[Dr.Web Ct](#)コマンドラインツールの `esconnect` [コマンド](#)を使用します。

接続するには、サーバーの証明書ファイルへのパスを指定して、`--Certificate` オプションを使用する必要があります。`--Login`と`--Password`パラメータを使用することで、ホストのID(集中管理サーバー上での表記は、端末の識別子)と集中管理サーバーの認証用パスワードも入力できます。この場合、サーバー



への接続は、正しいIDとパスワードのペアを指定した場合にのみ確立されます。パラメータが指定されない場合、サーバーへの接続は、(サーバーの設定に応じて、自動的またはアンチウイルスネットワークの管理者によって)サーバーで承認されている場合にのみ確立されます。

さらに、`--Newbie`オプション(新しいユーザーとして接続する)を使用することもできます。このモードがサーバーで許可されている場合、この接続が承認されると、サーバーは自動的に一意のIDとパスワードのペアを生成します。これはその後、このエージェントがサーバーに接続する際に使用されます。



このモードでは、すでにこのホストの別アカウントがサーバーに存在している場合でも、集中管理サーバーはそのホストの新しいアカウントを生成します。

Dr.Web for UNIX Internet Gatewaysに集中管理サーバーへの接続を指示するコマンドの標準的な例は次のとおりです。

```
# drweb-ctl esconnect <server address> --Certificate <path to the certificate file>
```

集中管理サーバーへの接続を確立すると、サーバーに設定されている権限とDr.Web ES AgentコンポーネントのMobileMode [設定パラメータ](#)の値に応じて、Dr.Web for UNIX Internet Gatewaysは集中管理モードまたはモバイルモードで動作します。無条件にモバイルモードを使用できるようにするには、パラメータの値をOnに設定します。集中管理モードで動作させるには、パラメータの値をOffに設定します。

集中管理サーバーに接続されているDr.Web for UNIX Internet Gatewaysにモバイルモードへの切り替えを指示するコマンドの標準的な例は次のとおりです。

```
# drweb-ctl cfset ESAgent.MobileMode On
```



使用する集中管理サーバーがモバイルモードをサポートしていない、または許可していない場合、MobileModeパラメータを調整してもDr.Web for UNIX Internet Gatewaysの動作をモバイルモードに切り替えることはできません。

集中管理サーバーから切断する方法

Dr.Web for UNIX Internet Gatewaysを集中管理サーバーから切断してその動作をスタンドアロンモードに切り替えるには、Dr.Web for UNIX Internet Gatewaysで提供される[Dr.Web Ctl](#)コマンドラインツールの `esdisconnect` [コマンド](#)を使用します。

```
# drweb-ctl esdisconnect
```

Dr.Web for UNIX Internet Gatewaysをスタンドアロンモードで使用するには、有効なライセンス[キーファイル](#)が必要です。それ以外の場合は、動作がスタンドアロンモードに切り替えられた後、Dr.Web for UNIX Internet Gatewaysのアンチウイルス機能が[ブロック](#)されます。

Dr.Web for UNIX Internet Gatewaysを有効化する方法

1. Doctor Web公式サイト<https://products.drweb.com/register/v4>から登録を実施します。
2. 登録時に指定したメールアドレスに、有効なライセンスキーファイルを含むアーカイブが送信されます(登録後にこのアーカイブをWebサイトから直接ダウンロードすることもできます)。



3. キーファイルの[インストール手順](#)を実行します。

Dr.Web for UNIX Internet Gatewaysをアップグレードする方法

コンポーネントのバージョンを[更新](#)するか、[新しいバージョンにアップグレード](#)してください。



アップグレード中に、現在のDr.Web for UNIX Internet Gatewaysバージョンを削除するように求められることがあります。

Dr.Web for UNIX Internet Gatewaysコンポーネントを追加または削除する方法

[コンポーネントのカスタムインストールとアンインストール](#)の手順に従います。



コンポーネントをインストール／アンインストールする場合、依存関係を解消するために他のDr.Web for UNIX Internet Gatewaysコンポーネントを追加でインストールまたはアンインストールする必要があります。

コンポーネント動作を管理する方法

Dr.Web for UNIX Internet Gatewaysコンポーネントのステータスを表示したり、それらの動作を管理したりするには、次のものを使用できます。

- [コマンドラインベース管理ツールDr.Web Ctl](#)(`drweb-ctl appinfo`、`drweb-ctl cfshow`、および `drweb-ctl cfset`コマンドを使用します。使用可能な管理コマンドのリストを表示するには、`drweb-ctl --help`コマンドを使用します)。
- Dr.Web for UNIX Internet Gatewaysの管理用[Webインターフェース](#)(デフォルトでは、Webブラウザから `https://127.0.0.1:4443/`にアクセスすると利用できます)。

Dr.Web for UNIX Internet Gatewaysのログを表示する方法

デフォルト設定に従って、すべてのDr.Web for UNIX Internet Gatewaysコンポーネントの一般ログは `syslog`ファイルに表示されます(システムコンポーネント `syslog`によってメッセージをログに記録するためのファイルはシステムによって異なり、ディレクトリ `/var/log`にあります)。一般ログ設定は、[設定ファイル](#)の `[Root]` [セクション](#)(`Log`パラメータと `DefaultLogLevel`パラメータ)で定義されます。設定セクションの各 [コンポーネント](#)には、`Log`パラメータと `LogLevel`パラメータがあります。それらのパラメータでログの保存場所と、コンポーネントがログに出力するメッセージのロギングレベルを設定します。

また、`drweb-ctl log`[コマンド](#)を使用することもできます。

ロギング設定を変更するには、コマンドライン管理ツールDr.Web CtlとDr.Web for UNIX Internet Gateways管理Webインターフェース(インストールされている場合)を使用してください。

- エラーを特定するために、すべてのコンポーネントのログの出力先を別のファイルに設定し、デバッグ情報がログに出力されるようにすることを推奨します。そのためには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.Log <path to log file>
# drweb-ctl cfset Root.DefaultLogLevel DEBUG
```



- デフォルトのロギング方法とログレベルに戻すには、次のコマンドを実行します。

```
# drweb-ctl cfset Root.Log -r  
# drweb-ctl cfset Root.DefaultLogLevel -r
```



Dr.Web for UNIX Internet Gatewaysコンポーネント

このセクションでは、Dr.Web for UNIX Internet Gatewaysのコンポーネントについて説明します。各コンポーネントの機能、動作原理、[設定ファイル](#)に保存されているパラメータに関する情報を確認できます。

Dr.Web ConfigD

Dr.Web ConfigD設定管理デーモンは、Dr.Web for UNIX Internet Gatewaysの主要な制御コンポーネントです。すべてのDr.Web for UNIX Internet Gatewaysコンポーネントの設定を一元的な環境に保存し、すべてのコンポーネントの動作を管理し、コンポーネント間で信頼できるデータのやり取りを整理します。

Dr.Web ConfigD設定管理デーモンは、次の機能を実行します。

- 設定に応じて、Dr.Web for UNIX Internet Gatewaysのコンポーネントを起動、停止する
- 障害が発生した場合にコンポーネントを自動的に再起動する
- 他のコンポーネントのリクエストに応じてコンポーネントを起動する
- 設定の変更時にコンポーネントに通知する
- 設定パラメータを一元管理するためのインターフェースを提供する
- 使用中のライセンスファイルの情報をコンポーネントに伝える
- コンポーネントのライセンス情報を受け入れる
- 専用コンポーネントから新しいライセンス情報を受け取る
- ライセンス情報の変更時に実行中のコンポーネントに通知する

動作原理

Dr.Web ConfigDコンポーネントは常にroot権限で実行されます。また、他のDr.Web for UNIX Internet Gatewaysコンポーネントを起動し、事前に開いていたソケットを介してそれらのコンポーネントと連携します。設定管理デーモンは、Dr.Web for UNIX Internet Gatewaysのその他のコンポーネントから、情報ソケット（すべてのコンポーネントがアクセス可能）および管理ソケット（root権限で実行されるコンポーネントのみがアクセス可能）を介して接続を受け入れることができます。また、ファイルから、または[Dr.Web ES Agent](#)を介して集中管理サーバーから設定とライセンスに関する情報を読み込みます。さらに、設定パラメータの正しいデフォルト値を設定します。いずれかのコンポーネントが起動するか、SIGHUPシグナルを受信するまでに、すべてのDr.Web for UNIX Internet Gatewaysコンポーネントの包括的で一貫性のある設定パラメーター式がDr.Web ConfigDに設定されます。

SIGHUPシグナルを受信すると、Dr.Web ConfigDは設定パラメータとライセンス情報を再度読み込みます。必要に応じて、デーモンはすべてのコンポーネント通知を送信して、設定を再度読み込むように指示します。

SIGTERMシグナルを受信すると、Dr.Web ConfigDはすべてのコンポーネントをシャットダウンした後、その動作を終了します。また、Dr.Web ConfigDはシャットダウン後、コンポーネントのすべての一時ファイルを削除します。



コンポーネントの連携の原則

1. 起動時に、すべてのコンポーネントはDr.Web ConfigDから設定パラメータとライセンスに関する情報を受け取ります。このパラメータのみが以降の操作で使用されます。
2. このデーモンは、管理されているすべてのコンポーネントから統合ログにメッセージを収集します。*stderr*コンポーネントに出力されたすべての情報は、Dr.Web ConfigDによって収集され、どのコンポーネントが出力したかを示すマークとともにDr.Web for UNIX Internet Gatewaysの統合ログに書き込まれます。
3. シャットダウンすると、管理されているコンポーネントは終了コードを返します。コードが101、102、または103ではない場合、設定デーモンはこのコンポーネントを再起動します。そのため、コンポーネントが異常終了すると再起動され、*stderr*からのエラーメッセージがDr.Web for UNIX Internet Gatewaysのログに登録されます。
 - **コード101**は、現在のライセンスでコンポーネントが動作できない場合に返されます。ライセンスパラメータを変更した後にのみ、コンポーネントが再起動されます。
 - **コード102**は、現在の設定パラメータでコンポーネントが動作できない場合に返されます。Dr.Web ConfigDは、設定パラメータが変更されたときにコンポーネントの再起動を試みます。
 - コード103は、Dr.Web ConfigDがリクエストに応じて起動したコンポーネント (**Dr.Web Scanning Engine**および**Dr.Web File Checker**) が長い間アイドル状態だった場合に返されます。コンポーネントがシャットダウンするまでの時間は、その設定で指定されます (*IdleTimeLimit*パラメータ)。
 - 設定管理デーモンから受け取った設定パラメータをオンザフライで適用できない場合、Dr.Web ConfigDがそれを再起動するように、コンポーネントはコード0で存在します。
 - コンポーネントが設定デーモンに接続できない、または通信プロトコルエラーが発生する場合、コンポーネントは*stderr*に適切なメッセージを出力し、コード1で終了します。
4. シグナル交換は次のように構成されています。
 - Dr.Web ConfigDはSIGHUPシグナルをコンポーネントに送信し、変更した設定パラメータを適用します。
 - Dr.Web ConfigDはSIGTERMシグナルをコンポーネントに送信し、コンポーネントをシャットダウンします。このシグナルを受信した後、コンポーネントは30秒後にシャットダウンします。
 - 30秒経ってもコンポーネントがシャットダウンしない場合、Dr.Web ConfigDはSIGKILLシグナルを送信して強制的にシャットダウンします。

コマンドライン引数

設定デーモンDr.Web ConfigDを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-configd [<parameters>]
```

設定デーモンDr.Web ConfigDは、以下のオプションを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了します。 短縮形：-h 引数：なし



<code>--version</code>	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了します。 短縮形： <code>-v</code> 引数：なし
<code>--config</code>	説明：指定した設定ファイルを今後の操作に使用します。 短縮形： <code>-c</code> 引数： <code><path to the file></code> - 使用する設定ファイルへのパス。
<code>--daemonize</code>	説明：コンポーネントをデーモンモードで実行します。 短縮形： <code>-d</code> 引数：なし
<code>--pid-file</code>	説明：指定されたPIDファイルを今後の操作に使用します。 短縮形： <code>-p</code> 引数： <code><path to the file></code> - プロセスID(PID)の保存先ファイルへのパス。

例：

```
$ /opt/drweb.com/bin/drweb-configd -d -c /etc/opt/drweb.com/drweb.ini
```

このコマンドはDr.Web ConfigDを、`/etc/opt/drweb.com/drweb.ini`の設定ファイルを使用するデーモンとして実行します。

スタートアップノート

Dr.Web for UNIX Internet Gatewaysの操作を有効にするには、Dr.Web ConfigDをデーモンとして実行する必要があります。通常は、Dr.Web ConfigDはOSの起動時に自動的に起動されます。そのため、Dr.Web ConfigDは、標準のOSディレクトリ(GNU/Linuxの場合は`/etc/init.d/`、FreeBSDの場合は`/usr/local/etc/rc.d/`)にある標準管理スクリプト`drweb-configd`と一緒に保存されます。コンポーネントの動作を管理するには、Dr.Web for UNIX Internet Gateways用のコマンドラインベース管理ツール[Dr.Web Ct](#)を使用できます(これは`drweb-ctl`コマンドを使用して呼び出されます)。



コマンドラインから製品のこのコンポーネントに関するドキュメントをリクエストするには、`man 1 drweb-configd`コマンドを使用します。

設定パラメータ

デーモンDr.Web ConfigDは、Dr.Web for UNIX Internet Gatewaysの統合された[設定ファイル](#)の[Root]セクションにある設定パラメータを使用します。

セクションには以下のパラメータが含まれています。

パラメータ	説明
<code>DefaultLogLevel</code> <code>{logging level}</code>	すべてのDr.Web for UNIX Internet Gatewaysコンポーネントについて、イベントロギングのデフォルトの ロギングレベル を定義します。



パラメータ	説明
	<p>このパラメータの値は、製品の中でロギングレベルを個別に設定できないすべてのコンポーネントに使用されます。</p> <p>デフォルト値: Notice</p>
LogLevel {logging level}	<p>Dr.Web ConfigDのイベントロギングのロギングレベル。</p> <p>デフォルト値: Notice</p>
Log {log type}	<p>設定デーモンのロギング方式と、このパラメータに別の値が指定されていないコンポーネントのロギング方式。</p> <p>設定ファイルが読み込まれる前の初回起動時に、設定デーモンは次のパラメータ値を使用します。</p> <ul style="list-style-type: none">• デーモンとして (-d オプションを付けて実行した場合) - SYSLOG: Daemon• その他の場合 - Stderr <p>コンポーネントがバックグラウンドモードで動作している(コマンドラインから -d オプションを使用して起動した)場合は、Stderrの値をこのパラメータに使用することはできません。</p> <p>デフォルト値: SYSLOG: Daemon</p>
PublicSocketPath {path to file}	<p>すべてのDr.Web for UNIX Internet Gatewaysコンポーネント間の通信に使用されるソケットへのパス。</p> <p>デフォルト値: /var/run/.com.drweb.public</p>
AdminSocketPath {path to file}	<p>昇格した(管理者の)権限を持つDr.Web for UNIX Internet Gatewaysコンポーネント間の通信に使用されるソケットへのパス。</p> <p>デフォルト値: /var/run/.com.drweb.admin</p>
CoreEnginePath {path to file}	<p>Dr.Web Virus-Finding Engineスキャンエンジンの動的ライブラリへのパス。</p> <p>デフォルト値: <var_dir>/lib/drweb32.dll</p> <ul style="list-style-type: none">• GNU/Linuxの場合: /var/opt/drweb.com/lib/drweb32.dll• FreeBSDの場合: /var/drweb.com/lib/drweb32.dll
VirusBaseDir {path to directory}	<p>ウイルスデータベースファイルがあるディレクトリへのパス。</p> <p>デフォルト値: <var_dir>/bases</p> <ul style="list-style-type: none">• GNU/Linuxの場合: /var/opt/drweb.com/bases• FreeBSDの場合: /var/drweb.com/bases
KeyPath {path to file}	<p>キーファイルへのパス(正規またはデモライセンス)。</p> <p>デフォルト値: <etc_dir>/drweb32.key</p> <ul style="list-style-type: none">• GNU/Linuxの場合: /etc/opt/drweb.com/drweb32.key• FreeBSDの場合: /usr/local/etc/drweb.com/drweb32.key
CacheDir {path to directory}	<p>キャッシュディレクトリへのパス(更新されたキャッシュとスキャンされたファイルに関する情報のキャッシュを保持するために使用されます)。</p>



パラメータ	説明
	デフォルト値 : <var_dir>/cache <ul style="list-style-type: none">• GNU/Linuxの場合 : /var/opt/drweb.com/cache• FreeBSDの場合 : /var/drweb.com/cache
TempDir <i>{path to directory}</i>	一時ファイルがあるディレクトリへのパス。 デフォルト値 : システム環境変数TMPDIR、TMP、TEMPまたはTMPDIRからコピーされたパス(環境変数はこの順序で検索されます)。これらの環境変数がない場合は、/tmp。
RunDir <i>{path to directory}</i>	実行中のコンポーネントが有するすべてのPIDファイルと、Dr.Web for UNIX Internet Gatewaysコンポーネント間の通信に使用されるソケットを含むディレクトリへのパス。 デフォルト値 : /var/run
VarLibDir <i>{path to directory}</i>	Dr.Web for UNIX Internet Gatewaysコンポーネントによって使用されるライブラリを含むディレクトリへのパス。 デフォルト値 : <var_dir>/lib <ul style="list-style-type: none">• GNU/Linuxの場合 : /var/opt/drweb.com/lib• FreeBSDの場合 : /var/drweb.com/lib
VersionDir <i>{path to directory}</i>	Dr.Web for UNIX Internet Gatewaysコンポーネントの現在のバージョンに関する情報が格納されているディレクトリへのパス。 デフォルト値 : <var_dir>/version <ul style="list-style-type: none">• GNU/Linuxの場合 : /var/opt/drweb.com/version• FreeBSDの場合 : /var/drweb.com/version
DwsDir <i>{path to directory}</i>	インターネットリソースカテゴリーの自動的に更新されるデータベースのファイルを含むディレクトリへのパス。 デフォルト値 : <var_dir>/dws <ul style="list-style-type: none">• GNU/Linuxの場合 : /var/opt/drweb.com/dws• FreeBSDの場合 : /var/drweb.com/dws
AdminGroup <i>{group name GID}</i>	Dr.Web for UNIX Internet Gateways管理用の管理者権限を持つユーザーのグループ。rootスーパーユーザーに加えて、これらのユーザーは、Dr.Web for UNIX Internet Gatewaysコンポーネントの権限をスーパーユーザー権限に昇格させることができます。 デフォルト値 : Dr.Web for UNIX Internet Gatewaysのインストール中に決定されます。
TrustedGroup <i>{group name GID}</i>	信頼するユーザーのグループ。このパラメータはネットワークトラフィックモニターコンポーネント(SpIDer Gate)の動作に使用されます。これらのユーザーのネットワークトラフィックはスキャンされずに、SpIDer Gateによってスキップされます。 ここに存在しないグループを指定することはできません。その場合、SpIDer Gateは起動に失敗します。



パラメータ	説明
	パラメータの値がない場合は、SpIDer Gate設定のOutputDivertパラメータにAuto値を指定することはできません。 デフォルト値: drweb
DebugIpc {Boolean}	詳細をデバッグレベルでログファイルに含めます (LogLevel = DEBUGの場合など)。IPCメッセージは、設定デーモンと他のコンポーネントとの間のやり取りを示します。 デフォルト値: No
UseCloud {Boolean}	悪意のあるファイルやURLに関する情報を受け取るためにDr.Web Cloudサービスを使用するかどうかを設定します。 デフォルト値: No
AntispamCorePath {path to file}	このパラメータは使用されません。 デフォルト値: <var_dir>/lib/vaderetro.so • GNU/Linuxの場合: /var/opt/drweb.com/lib/vaderetro.so • FreeBSDの場合: /var/drweb.com/lib/vaderetro.so
VersionNotification {Boolean}	現在インストールされているDr.Web for UNIX Internet Gatewaysバージョンのアップデートが利用可能であることをユーザーに通知します。 デフォルト値: Yes
UseVxcube {Boolean}	MTAに接続された外部フィルターのモードで、メール添付ファイルの解析にDr.Web vxCubeを使用します。 デフォルト値: No
VxcubeApiAddress {string}	Dr.Web vxCube APIサーバーが稼働しているホストのドメイン名 (FQDN) またはIPアドレス。 デフォルト値: (未設定)
VxcubeApiKey {string}	Dr.Web vxCubeのAPIキー。 デフォルト値: (未設定)
VxcubeProxyUrl {connection address}	Dr.Web vxCubeへの接続に使用されるプロキシサーバーのアドレス。 認証のないHTTPプロキシにのみ対応しています。 以下の値を使用できます。<connection address> - http:// <host>:<port>のフォーマットで示したプロキシサーバーの接続パラメータ。ここで、 • <host>はプロキシサーバーのホストアドレスです (IPアドレスまたはドメイン名、つまりFQDN)。 • <port>は使用するポートです。 デフォルト値: (未設定)



Dr.Web Ctl

このセクションの内容

- [概要](#)
- [リモートホストスキャン](#)

概要

特別なDr.Web Ctlユーティリティ(`drweb-ctl`)を使用することで、OSのコマンドラインからDr.Web for UNIX Internet Gatewaysの動作を管理できます。このユーティリティを使用して次の動作を実行できます。

- ブートレコードを含む、ファイルシステムオブジェクトのスキャンを開始する
- リモートネットワークホストでファイルのスキャンを開始する([下記](#)の注意を参照)
- アンチウイルスコンポーネント(ディストリビューションに応じてウイルスデータベース、スキャンエンジンなど)の更新を開始する
- Dr.Web for UNIX Internet Gateways設定のパラメータを確認・変更する
- Dr.Web for UNIX Internet Gatewaysコンポーネントのステータスや検出された脅威に関する統計を確認する
- 集中管理サーバーに接続、または集中管理サーバーとの接続を切断する
- 隔離を表示し、隔離されたオブジェクトを管理する([Dr.Web File Checker](#)コンポーネント経由で)
- 集中管理サーバーに接続、または集中管理サーバーとの接続を切断する

Dr.Web for UNIX Internet Gatewaysを管理するためのユーザーコマンドは、[Dr.Web ConfigD](#)設定デーモンの動作中にのみ適用されます(デフォルトでは、このコンポーネントはシステム起動時に自動的に起動します)。



一部のコントロールコマンドはスーパーユーザー権限を必要とします。

権限を昇格させるには`su`コマンド(カレントユーザーを変更する)または`sudo`コマンド(指定したコマンドを他のユーザーの権限で実行する)を使用します。

`drweb-ctl`ツールは、Dr.Web for UNIX Internet Gatewaysの動作を管理するコマンドの自動補完をサポートしています(コマンドシェル内でこのオプションが有効になっている場合)。コマンドシェルが自動補完を許可していない場合、このオプションの設定を行うことができます。方法については、お使いのOSディストリビューションのマニュアルを参照してください。



シャットダウンする際、ツールはPOSIX準拠システムの表記規則に従って終了コードを返します。操作が正常に完了した場合は0(ゼロ)、それ以外の場合は0(ゼロ)以外です。

ツールが0以外 (non-null) の終了コードを返すのは、内部エラーの場合のみであるという点に注意してください(ツールがコンポーネントに接続できなかった、リクエストされた操作を実行できなかったなど)。ツールが脅威を検出(そして駆除)した場合は、リクエストされた操作(scanなど)が正常に実行されたため、0(null) 終了コードを返します。検出された脅威と適用されたアクションのリストを明らかにする必要がある場合、コンソールに表示されたメッセージを分析してください。

すべてのエラーのコードについては、[付録F. 既知のエラー](#)のセクションのリストをご確認ください。

リモートホストスキャン

Dr.Web for UNIX Internet Gatewaysを使用して、リモートネットワークホストにあるファイルの脅威に対するスキャンを実行できます。このようなホストには、フルコンピューティングマシン(ワークステーションやサーバーなど)だけでなく、ルーター、セットトップボックス、いわゆるモノのインターネット(IoT)と呼ばれるその他のスマートデバイスも含まれます。リモートスキャンを実行するには、リモートホストがSSH(セキュアシェル)またはTelnetを介したリモート端末アクセスを提供する必要があります。デバイスにアクセスするには、リモートホストのIPアドレスとドメイン名、SSHまたはTelnetを介してリモートでシステムにアクセスするユーザーの認証情報を知っている必要があります。このユーザーは、スキャン済みファイルへのアクセス権限(少なくとも読み取り権限)を持っている必要があります。

この機能は、リモートホスト上の悪意のあるファイルや疑わしいファイルの検出にのみ使用できます。リモートスキャンの手段を用いた脅威の排除(すなわち、悪意のあるオブジェクトの隔離への移動、削除および修復)はできません。リモートホストで検出された脅威を排除するには、このホストによって直接提供される管理ツールを使用する必要があります。たとえば、ルーターやその他のスマートデバイスの場合は、ファームウェア更新のメカニズムを使用できます。コンピューティングマシンの場合は、コンピューティングマシンへの接続(任意でリモート端末モードを使用)とファイルシステムのそれぞれの操作(ファイルの削除または移動など)、またはコンピューティングマシンにインストールされているアンチウイルスソフトウェアの実行を介して実行できます。

リモートスキャンはコマンドラインツールdrweb-ctlからのみ実行できます(remotescanコマンドを使用します)。



コマンドライン呼び出しフォーマット

1. 製品を管理するためのコマンドラインユーティリティを呼び出すコマンドフォーマット

Dr.Web for UNIX Internet Gatewaysの動作を管理するコマンドラインツールの呼び出しフォーマットは以下のとおりです。

```
$ drweb-ctl [<general options> | <command> [<argument>] [<command options>]]
```

各パラメータは次のとおりです。

- *<general options>* - コマンドが指定されていない場合に起動時に適用できる、またはあらゆるコマンドにおいて適用できるオプションです。起動時に必須ではありません。
- *<command>* - Dr.Web for UNIX Internet Gatewaysによって実行されるコマンド(スキャンの開始、隔離されたオブジェクトのリストの出力など)です。
- *<argument>* - コマンド引数です。指定されたコマンドに依存します。コマンドによってはない場合もあります。
- *<command options>* - 指定されたコマンドの動作を管理するためのオプションです。一部のコマンドでは省略できます。

2. 全般的なオプション

以下の全般的なオプションを使用できます。

オプション	説明
-h, --help	全般的なヘルプ情報を表示して終了します。いずれかのコマンドに関するヘルプ情報を表示させるには、以下の呼び出しを使用します。 <pre>\$ drweb-ctl <command> -h</pre>
-v, --version	モジュールバージョンに関する情報を表示して終了します。
-d, --debug	指定されたコマンドの実行時にデバッグ情報を表示します。コマンドが指定されていない場合は実行できません。以下の呼び出しを使用します。 <pre>\$ drweb-ctl <command> -d</pre>

3. コマンド

Dr.Web for UNIX Internet Gatewaysを管理するコマンドは以下のグループに分けることができます。

- [アンチウイルススキャン](#)のコマンド
- [更新を管理し](#)、集中管理モードでの動作を管理するコマンド
- [設定を管理する](#)コマンド



- [検出された脅威および隔離を管理するコマンド](#)
- [情報に関するコマンド](#)



コマンドラインから製品のこのコンポーネントに関するヘルプを要求するには、`man 1 drweb-ctl1`のコマンドを使用します。

3.1. アンチウイルススキャンのコマンド

アンチウイルススキャンを管理するコマンドには以下のものがあります。

コマンド	説明
<code>scan <path></code>	<p>機能 : ファイルスキャンコンポーネント Dr.Web File Checker による、指定されたファイルまたはディレクトリのスキャンを開始します。</p> <p>引数</p> <p><code><path></code> - スキャンするファイルまたはディレクトリへのパスです (パスは相対パスでも可)。</p> <p><code>--stdin</code> または <code>--stdin0</code> オプションを使用する場合、この引数は省略できます。特定の条件を満たす複数のファイルを指定するには、<code>find</code> コーティリティ (使用例 参照) および <code>--stdin</code> または <code>--stdin0</code> オプションを使用します。</p> <p>オプション</p> <p><code>-a</code> [<code>--Autonomous</code>] は、指定されたスキャンを実行し、完了後にそれらを終了させるために、Dr.Web Scanning Engine と Dr.Web File Checker の自律コピーを実行します。自律コピーによるスキャン中に検出された脅威は、<code>threats</code> コマンドによって表示される、検出された脅威のリストに追加されず (下記 参照)、それらの脅威に関する情報は集中管理サーバーには送信されません (Dr.Web for UNIX Internet Gateways が集中管理サーバーで管理されている場合)。</p> <p><code>--stdin</code> - スキャンのためのパスのリストを標準的な入力文字列 (<code>stdin</code>) から取得します。リスト内のパスは改行文字 (<code>\n</code>) で区切られている必要があります。</p> <p><code>--stdin0</code> - スキャンのためのパスのリストを標準的な入力文字列 (<code>stdin</code>) から取得します。リスト内のパスはヌル文字 (<code>\0</code>) で区切られている必要があります。</p> <div data-bbox="606 1590 1436 1825"><p> <code>--stdin</code> および <code>--stdin0</code> オプションを使用する場合、リストのパスに検索のパターンまたは正規表現を含めることはできません。<code>--stdin</code> および <code>--stdin0</code> オプションを使用して、外部ユーティリティ (<code>scan</code> コマンドの <code>find</code> など) によって生成されるパスリストを処理することをお勧めします (使用例 を参照)。</p></div> <p><code>--Exclude <path></code> - 除外するパスです。パスは相対パスにすることができ、ファイルマスクを含むことができます (ワイルドカード「<code>?</code>」と「<code>*</code>」、シンボルクラス「<code>[]</code>」、「<code>[!]</code>」、「<code>[^]</code>」を使用できます)。</p> <p>任意オプション、複数回設定できます。</p>



コマンド	説明
	<p><code>--Report <type></code> - スキャンレポートのタイプを指定します。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• BRIEF - 短いレポート• DEBUG - 詳細なレポート• JSON - JSON形式のシリアル化されたレポート <p>デフォルト値: BRIEF</p> <p><code>--ScanTimeout <number></code> - 1つのファイルをスキャンする際のタイムアウトをミリ秒で指定します。</p> <p>値に0が指定された場合、スキャンにかかる時間は制限されません。</p> <p>デフォルト値: 0</p> <p><code>--PackerMaxLevel <number></code> - 圧縮されたオブジェクトをスキャンする際のネスティングレベルの上限を指定します。圧縮されたオブジェクトは、特別なソフトウェア (UPX、PELock、PECompact、Petite、ASPack、Morphineなど) で圧縮された実行コードです。そのようなオブジェクトには、圧縮されたオブジェクトなども含む他の圧縮されたオブジェクトが含まれる場合があります。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他の圧縮されたオブジェクト内の圧縮されたオブジェクトはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値: 8</p> <p><code>--ArchiveMaxLevel <number></code> - 他のアーカイブが含まれる可能性のあるアーカイブ (zip、rarなど) をスキャンするときの最大ネスティングレベルを設定します (これらのアーカイブには他のアーカイブなどが含まれる場合もあります)。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他のアーカイブ内のアーカイブはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値: 8</p> <p><code>--MailMaxLevel <number></code> - 他のファイルが含まれる可能性のあるメーラーのファイル (pst、tbbなど) をスキャンするときの最大ネスティングレベルを設定します (これらのファイルには他のファイルなどが含まれる場合もあります)。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他のオブジェクト内のオブジェクトはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値: 8</p> <p><code>--ContainerMaxLevel <number></code> - 他のオブジェクトが含まれる他のタイプのオブジェクト (HTMLページ、jarファイルなど) をスキャンするときの最大ネスティングレベルを設定します。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他のオブジェクト内のオブジェクトはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値: 8</p> <p><code>--MaxCompressionRatio <ratio></code> - スキャンされるオブジェクトの最大圧縮率を指定します。</p>



コマンド	説明
	<p>値は2以上にする必要があります。</p> <p>デフォルト値: 3000</p> <p>--MaxSizeToExtract <i><size></i> - アーカイブに含まれるファイルの最大サイズを指定します。このパラメータの値よりサイズが大きいファイルは、スキャン時にスキップされます。デフォルトでは、アーカイブ内のファイルのサイズ制限はありません。サイズは、サフィックス(b、kb、mb、gb)を付けた数値で指定します。サフィックスが指定されていない場合、値はバイト単位のサイズとして扱われます。</p> <p>デフォルト値: なし</p> <p>--HeuristicAnalysis <i><On/Off></i> - スキャン中のヒューリスティック解析を有効または無効にします。</p> <p>デフォルト値: On</p> <p>--OnKnownVirus <i><action></i> - シグネチャベースの解析を使用して検出された既知の脅威に対して適用されるアクションです。</p> <p>可能なアクション: Report、Cure、Quarantine、Delete</p> <p>デフォルト値: Report</p> <p>--OnIncurable <i><action></i> - 修復不可能な脅威が検出された場合、または修復アクション(Cure)が失敗した場合に適用されるアクションです。</p> <p>可能なアクション: Report、Quarantine、Delete</p> <p>デフォルト値: Report</p> <p>--OnSuspicious <i><action></i> - ヒューリスティック解析によって検出された疑わしいオブジェクトに対して適用されるアクションです。</p> <p>可能なアクション: Report、Quarantine、Delete</p> <p>デフォルト値: Report</p> <p>--OnAdware <i><action></i> - 検出されたアドウェアに対して適用されるアクションです。</p> <p>可能なアクション: Report、Quarantine、Delete</p> <p>デフォルト値: Report</p> <p>--OnDialers <i><action></i> - 検出されたダイヤラーに対して適用されるアクションです。</p> <p>可能なアクション: Report、Quarantine、Delete</p> <p>デフォルト値: Report</p> <p>--OnJokes <i><action></i> - 検出されたジョークプログラムに対して適用されるアクションです。</p> <p>可能なアクション: Report、Quarantine、Delete</p> <p>デフォルト値: Report</p> <p>--OnRiskware <i><action></i> - 検出されたリスクウェアに対して適用されるアクションです。</p> <p>可能なアクション: Report、Quarantine、Delete</p> <p>デフォルト値: Report</p> <p>--OnHacktools <i><action></i> - 検出されたハッキングツールに対して適用されるアクションです。</p> <p>可能なアクション: Report、Quarantine、Delete</p>



コマンド	説明
	<p>デフォルト値 : Report</p> <div data-bbox="609 309 1449 488" style="border: 1px solid #ccc; background-color: #e6f2e6; padding: 10px;"> コンテナ (アーカイブ、メールメッセージなど) 内のファイルで脅威が検出された場合は、ファイルを削除するアクション (Delete) の代わりにコンテナの隔離への移動 (Quarantine) が実行されます。</div> <p>--FollowSymlinks - シンボリックリンクを自動的に解決します。</p>
bootscan <disk drive> ALL	<p>機能 : ファイルスキャンコンポーネント Dr.Web File Checker を介して、指定されたディスク上のブートレコードのスキャンを開始します。MBRとVBRの両方のレコードがスキャンされます。</p> <p>引数</p> <p><disk drive> - ブートレコードをスキャンするディスクデバイスのブロックファイルへのパス。スペースで区切って複数のディスクデバイスを指定できます。引数は必須です。デバイスファイルの代わりに ALL を指定した場合は、使用可能なすべてのディスクデバイスにあるすべてのブートレコードが確認されます。</p> <p>オプション</p> <p>-a [--Autonomous] は、指定されたスキャンを実行し、完了後にそれらを終了させるために、Dr.Web Scanning Engine と Dr.Web File Checker の自律コピーを実行します。自律コピーによるスキャン中に検出された脅威は、threats コマンドによって表示される、検出された脅威のリストに追加されず (下記参照)、それらの脅威に関する情報は集中管理サーバーには送信されません (Dr.Web for UNIX Internet Gateways が集中管理サーバーで管理されている場合)。</p> <p>--Report <type> - スキャンレポートのタイプを指定します。</p> <p>使用可能な値 :</p> <ul style="list-style-type: none">• BRIEF - 短いレポート• DEBUG - 詳細なレポート• JSON - JSON形式のシリアル化されたレポート <p>デフォルト値 : BRIEF</p> <p>--ScanTimeout <number> - 1つのファイルをスキャンする際のタイムアウトをミリ秒で指定します。</p> <p>値に 0 が指定された場合、スキャンにかかる時間は制限されません。</p> <p>デフォルト値 : 0</p> <p>--HeuristicAnalysis <On/Off> - スキャン中のヒューリスティック解析を有効または無効にします。</p> <p>デフォルト値 : On</p> <p>--Cure <Yes/No> - 脅威が検出された際に修復を試みる動作を有効または無効にします。</p> <p>値に No が指定された場合、検出された脅威に関する通知のみが表示されます。</p> <p>デフォルト値 : No</p>



コマンド	説明
proscan	<p data-bbox="566 248 1449 315">--ShellTrace - ブートレコードをスキャンする際の、追加のデバッグ情報の表示を有効にします。</p> <p data-bbox="566 338 1449 465">機能 : Dr.Web File Checkerコンポーネントによる、現在実行中のシステムプロセスのコードを含んだ実行ファイルのスキャンを開始します。悪意のある実行ファイルが検出された場合、それらは駆除され、そのファイルによって実行されたすべてのプロセスを強制的に終了します。</p> <p data-bbox="566 499 699 528">引数 : なし</p> <p data-bbox="566 562 683 591">オプション</p> <p data-bbox="566 618 1449 842">-a [--Autonomous]は、指定されたスキャンを実行し、完了後にそれらを終了させるために、Dr.Web Scanning EngineとDr.Web File Checkerの自律コピーを実行します。自律コピーによるスキャン中に検出された脅威は、threatsコマンドによって表示される、検出された脅威のリストに追加されず(下記参照)、それらの脅威に関する情報は集中管理サーバーには送信されません(Dr.Web for UNIX Internet Gatewaysが集中管理サーバーで管理されている場合)。</p> <p data-bbox="566 853 1257 882">--Report <type> - スキャンレポートのタイプを指定します。</p> <p data-bbox="608 904 799 934">使用可能な値 :</p> <ul data-bbox="608 945 1150 1066" style="list-style-type: none">• BRIEF - 短いレポート• DEBUG - 詳細なレポート• JSON - JSON形式のシリアル化されたレポート <p data-bbox="608 1084 847 1113">デフォルト値 : BRIEF</p> <p data-bbox="566 1133 1449 1200">--ScanTimeout <number> - 1つのファイルをスキャンする際のタイムアウトをミリ秒で指定します。</p> <p data-bbox="608 1211 1374 1240">値に0が指定された場合、スキャンにかかる時間は制限されません。</p> <p data-bbox="608 1256 783 1285">デフォルト値 : 0</p> <p data-bbox="566 1305 1449 1373">--HeuristicAnalysis <On/Off> - スキャン中のヒューリスティック解析を有効または無効にします。</p> <p data-bbox="608 1384 799 1413">デフォルト値 : On</p> <p data-bbox="566 1433 1449 1648">--PackerMaxLevel <number> - 圧縮されたオブジェクトをスキャンする際のネスティングレベルの上限を指定します。圧縮されたオブジェクトは、特別なソフトウェア(UPX、PELock、PECompact、Petite、ASPack、Morphineなど)で圧縮された実行コードです。そのようなオブジェクトには、圧縮されたオブジェクトなども含む他の圧縮されたオブジェクトが含まれる場合があります。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他の圧縮されたオブジェクト内の圧縮されたオブジェクトはスキャンされません。</p> <p data-bbox="608 1659 1449 1727">値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p data-bbox="608 1738 783 1767">デフォルト値 : 8</p> <p data-bbox="566 1787 1449 1854">--OnKnownVirus <action> - シグネチャベースの解析を使用して検出された既知の脅威に対して適用されるアクションです。</p> <p data-bbox="608 1865 1294 1895">可能なアクション : Report、Cure、Quarantine、Delete</p> <p data-bbox="608 1910 863 1939">デフォルト値 : Report</p> <p data-bbox="566 1960 1449 2027">--OnIncurable <action> - 修復不可能な脅威が検出された場合、または修復アクション(Cure)が失敗した場合に適用されるアクションです。</p>



コマンド	説明
	<p>可能なアクション: Report、Quarantine、Delete デフォルト値: Report</p> <p>--OnSuspicious <action> - ヒューリスティック解析によって検出された疑わしいオブジェクトに対して適用されるアクションです。</p> <p>可能なアクション: Report、Quarantine、Delete デフォルト値: Report</p> <p>--OnAdware <action> - 検出されたアドウェアに対して適用されるアクションです。</p> <p>可能なアクション: Report、Quarantine、Delete デフォルト値: Report</p> <p>--OnDialers <action> - 検出されたダイヤラーに対して適用されるアクションです。</p> <p>可能なアクション: Report、Quarantine、Delete デフォルト値: Report</p> <p>--OnJokes <action> - 検出されたジョークプログラムに対して適用されるアクションです。</p> <p>可能なアクション: Report、Quarantine、Delete デフォルト値: Report</p> <p>--OnRiskware <action> - 検出されたリスクウェアに対して適用されるアクションです。</p> <p>可能なアクション: Report、Quarantine、Delete デフォルト値: Report</p> <p>--OnHacktools <action> - 検出されたハッキングツールに対して適用されるアクションです。</p> <p>可能なアクション: Report、Quarantine、Delete デフォルト値: Report</p> <div data-bbox="608 1368 1449 1509" style="border: 1px solid #ccc; background-color: #e6f2e6; padding: 10px; margin-top: 10px;"> 実行ファイルで脅威が検出された場合、Dr.Web for UNIX Internet Gatewaysは、そのファイルによって開始されたすべてのプロセスを終了するという点に注意してください。</div>
netscan [<i><path></i>]	<p>機能 : ネットワークデータスキャン用の Dr.Web Network Checker エージェントを介して、指定されたファイルまたはディレクトリの分散スキャンを開始します。UNIX向けDr.Webが動作している他のホストへの接続が設定されていない場合、スキャンはローカルで利用可能なスキャンエンジン経由でのみ実行されず (scanコマンドと同様)。</p> <p>引数</p> <p><path> - スキャンするファイルまたはディレクトリへのパスです。</p> <p>この引数が指定されていない場合、入力スレッドstdinを介して受信したデータがスキャンされます。</p> <p>オプション</p> <p>--Report <type> - スキャンレポートのタイプを指定します。</p>



コマンド	説明
	<p>使用可能な値:</p> <ul style="list-style-type: none">• BRIEF - 短いレポート• DEBUG - 詳細なレポート• JSON - JSON形式のシリアル化されたレポート <p>デフォルト値: BRIEF</p> <p>--ScanTimeout <number> - 1つのファイルをスキャンする際のタイムアウトをミリ秒で指定します。</p> <p>値に0が指定された場合、スキャンにかかる時間は制限されません。</p> <p>デフォルト値: 0</p> <p>--HeuristicAnalysis <On/Off> - スキャン中のヒューリスティック解析を有効または無効にします。</p> <p>デフォルト値: On</p> <p>--PackerMaxLevel <number> - 圧縮されたオブジェクトをスキャンする際のネスティングレベルの上限を指定します。圧縮されたオブジェクトは、特別なソフトウェア (UPX、PELock、PECompact、Petite、ASPack、Morphineなど) で圧縮された実行コードです。そのようなオブジェクトには、圧縮されたオブジェクトなども含む他の圧縮されたオブジェクトが含まれる場合があります。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他の圧縮されたオブジェクト内の圧縮されたオブジェクトはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値: 8</p> <p>--ArchiveMaxLevel <number> - 他のアーカイブが含まれる可能性のあるアーカイブ (zip、rarなど) をスキャンするときの最大ネスティングレベルを設定します (これらのアーカイブには他のアーカイブなどが含まれる場合もあります)。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他のアーカイブ内のアーカイブはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値: 8</p> <p>--MailMaxLevel <number> - 他のファイルが含まれる可能性のあるメールのファイル (pst、tbbなど) をスキャンするときの最大ネスティングレベルを設定します (これらのファイルには他のファイルなどが含まれる場合もあります)。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他のオブジェクト内のオブジェクトはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値: 8</p> <p>--ContainerMaxLevel <number> - 他のオブジェクトが含まれる他のタイプのオブジェクト (HTMLページ、jarファイルなど) をスキャンするときの最大ネスティングレベルを設定します。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他のオブジェクト内のオブジェクトはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値: 8</p>



コマンド	説明
	<p><code>--MaxCompressionRatio <ratio></code> - スキャンされるオブジェクトの最大圧縮率を指定します。</p> <p>値は2以上にする必要があります。</p> <p>デフォルト値: 3000</p> <p><code>--MaxSizeToExtract <size></code> - アーカイブに含まれるファイルの最大サイズを指定します。このパラメータの値よりサイズが大きいファイルは、スキャン時にスキップされます。デフォルトでは、アーカイブ内のファイルのサイズ制限はありません。サイズは、サフィックス(b、kb、mb、gb)を付けた数値で指定します。サフィックスが指定されていない場合、値はバイト単位のサイズとして扱われます。</p> <p>デフォルト値: なし</p> <p><code>--Cure <Yes/No></code> - 脅威が検出された際に修復を試みる動作を有効または無効にします。</p> <p>値にNoが指定された場合、検出された脅威に関する通知のみが表示されます。</p> <p>デフォルト値: No</p>
<code>flowscan <path></code>	<p>機能: 「flow」メソッドを使用して、指定されたファイルまたはディレクトリのスキャンを、Dr.Web File Checkerを介して開始します。</p> <div data-bbox="608 976 1449 1099" style="border: 1px solid #ccc; background-color: #fff9c4; padding: 10px;"><p> ファイルやディレクトリのオンデマンドスキャンには、<code>scan</code>コマンドを使用することをお勧めします。</p></div> <p>引数</p> <p><code><path></code> - スキャンするファイルまたはディレクトリへのパスです。</p> <p>オプション</p> <p><code>--ScanTimeout <number></code> - 1つのファイルをスキャンする際のタイムアウトをミリ秒で指定します。</p> <p>値に0が指定された場合、スキャンにかかる時間は制限されません。</p> <p>デフォルト値: 0</p> <p><code>--HeuristicAnalysis <On/Off></code> - スキャン中のヒューリスティック解析を有効または無効にします。</p> <p>デフォルト値: On</p> <p><code>--PackerMaxLevel <number></code> - 圧縮されたオブジェクトをスキャンする際のネスティングレベルの上限を指定します。圧縮されたオブジェクトは、特別なソフトウェア(UPX、PELock、PECompact、Petite、ASPack、Morphineなど)で圧縮された実行コードです。そのようなオブジェクトには、圧縮されたオブジェクトなども含む他の圧縮されたオブジェクトが含まれる場合があります。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他の圧縮されたオブジェクト内の圧縮されたオブジェクトはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値: 8</p> <p><code>--ArchiveMaxLevel <number></code> - 他のアーカイブが含まれる可能性のあるアーカイブ(zip、rarなど)をスキャンするときの最大ネスティングレベルを設定</p>



コマンド	説明
	<p>します（これらのアーカイブには他のアーカイブなどが含まれる場合もあります）。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他のアーカイブ内のアーカイブはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値：8</p> <p>--MailMaxLevel <number> - 他のファイルが含まれる可能性のあるメーラーのファイル（pst、tbbなど）をスキャンするときの最大ネスティングレベルを設定します（これらのファイルには他のファイルなどが含まれる場合もあります）。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他のオブジェクト内のオブジェクトはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値：8</p> <p>--ContainerMaxLevel <number> - 他のオブジェクトが含まれる他のタイプのオブジェクト（HTMLページ、jarファイルなど）をスキャンするときの最大ネスティングレベルを設定します。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他のオブジェクト内のオブジェクトはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値：8</p> <p>--MaxCompressionRatio <ratio> - スキャンされるオブジェクトの最大圧縮率を指定します。</p> <p>値は2以上にする必要があります。</p> <p>デフォルト値：3000</p> <p>--OnKnownVirus <action> - シグネチャベースの解析を使用して検出された既知の脅威に対して適用されるアクションです。</p> <p>可能なアクション：Report、Cure、Quarantine、Delete</p> <p>デフォルト値：Report</p> <p>--OnIncurable <action> - 修復不可能な脅威が検出された場合、または修復アクション（Cure）が失敗した場合に適用されるアクションです。</p> <p>可能なアクション：Report、Quarantine、Delete</p> <p>デフォルト値：Report</p> <p>--OnSuspicious <action> - ヒューリスティック解析によって検出された疑わしいオブジェクトに対して適用されるアクションです。</p> <p>可能なアクション：Report、Quarantine、Delete</p> <p>デフォルト値：Report</p> <p>--OnAdware <action> - 検出されたアドウェアに対して適用されるアクションです。</p> <p>可能なアクション：Report、Quarantine、Delete</p> <p>デフォルト値：Report</p> <p>--OnDialers <action> - 検出されたダイヤラーに対して適用されるアクションです。</p>




コマンド	説明
	<p>可能なアクション: Report、Quarantine、Delete デフォルト値: Report</p> <p>--OnJokes <action> - 検出されたジョークプログラムに対して適用されるアクションです。</p> <p>可能なアクション: Report、Quarantine、Delete デフォルト値: Report</p> <p>--OnRiskware <action> - 検出されたリスクウェアに対して適用されるアクションです。</p> <p>可能なアクション: Report、Quarantine、Delete デフォルト値: Report</p> <p>--OnHacktools <action> - 検出されたハッキングツールに対して適用されるアクションです。</p> <p>可能なアクション: Report、Quarantine、Delete デフォルト値: Report</p> <div data-bbox="608 857 1449 1048" style="background-color: #e6f2e6; padding: 10px;"> コンテナ (アーカイブ、メールメッセージなど) 内のファイルで脅威が検出された場合は、ファイルを削除するアクション (Delete) の代わりにコンテナの隔離への移動 (Quarantine) が実行されます。</div>
rawscan <path>	<p>機能: Dr.Web File Checkerを使用せずに、指定されたファイルまたはディレクトリのDr.Web Scanning Engineによる「raw」スキャンを直接開始します。</p> <div data-bbox="608 1171 1449 1637" style="background-color: #fff9c4; padding: 10px;"> 「raw」スキャンで検出された脅威はthreatsコマンドで表示される、検出された脅威のリストには含まれないということに注意してください (下記参照)。</div> <p>このコマンドは、Dr.Web Scanning Engineの機能をデバッグするためにのみ使用することをお勧めします。ファイル内で検出された脅威のうち少なくとも1つの脅威が駆除されている場合、コマンドは「cured」(修復済み)ステータスを出力します (すべての脅威が駆除されているとは限りません)。そのため、徹底的なファイルスキャンが必要な場合にこのコマンドを使用することは <i>お勧めできません</i>。その場合、scanコマンドを使用することをお勧めします。</p> <p>引数</p> <p><path> - スキャンするファイルまたはディレクトリへのパスです。</p> <p>オプション</p> <p>--ScanEngine <path> - Dr.Web Scanning EngineのUNIXソケットへのパスです。指定していない場合、スキャンエンジンの自律インスタンスが開始されます (スキャンが完了するとシャットダウンされます)。</p> <p>--Report <type> - スキャンレポートのタイプを指定します。</p>



コマンド	説明
	<p>使用可能な値:</p> <ul style="list-style-type: none">• BRIEF - 短いレポート• DEBUG - 詳細なレポート• JSON - JSON形式のシリアル化されたレポート <p>デフォルト値: BRIEF</p> <p><code>--ScanTimeout <number></code> - 1つのファイルをスキャンする際のタイムアウトをミリ秒で指定します。</p> <p>値に0が指定された場合、スキャンにかかる時間は制限されません。</p> <p>デフォルト値: 0</p> <p><code>--PackerMaxLevel <number></code> - 圧縮されたオブジェクトをスキャンする際のネスティングレベルの上限を指定します。圧縮されたオブジェクトは、特別なソフトウェア (UPX、PELock、PECompact、Petite、ASPack、Morphineなど) で圧縮された実行コードです。そのようなオブジェクトには、圧縮されたオブジェクトなども含む他の圧縮されたオブジェクトが含まれる場合があります。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他の圧縮されたオブジェクト内の圧縮されたオブジェクトはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値: 8</p> <p><code>--ArchiveMaxLevel <number></code> - 他のアーカイブが含まれる可能性のあるアーカイブ (zip、rarなど) をスキャンするときの最大ネスティングレベルを設定します (これらのアーカイブには他のアーカイブなどが含まれる場合もあります)。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他のアーカイブ内のアーカイブはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値: 8</p> <p><code>--MailMaxLevel <number></code> - 他のファイルが含まれる可能性のあるメーラーのファイル (pst、tbbなど) をスキャンするときの最大ネスティングレベルを設定します (これらのファイルには他のファイルなどが含まれる場合もあります)。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他のオブジェクト内のオブジェクトはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値: 8</p> <p><code>--ContainerMaxLevel <number></code> - 他のオブジェクトが含まれる他のタイプのオブジェクト (HTMLページ、jarファイルなど) をスキャンするときの最大ネスティングレベルを設定します。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他のオブジェクト内のオブジェクトはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値: 8</p> <p><code>--MaxCompressionRatio <ratio></code> - スキャンされるオブジェクトの最大圧縮率を指定します。</p> <p>値は2以上にする必要があります。</p>



コマンド	説明
	<p>デフォルト値 : 3000</p> <p>--MaxSizeToExtract <size> - アーカイブに含まれるファイルの最大サイズを指定します。このパラメータの値よりサイズが大きいファイルは、スキャン時にスキップされます。デフォルトでは、アーカイブ内のファイルのサイズ制限はありません。サイズは、サフィックス(b, kb, mb, gb)を付けた数値で指定します。サフィックスが指定されていない場合、値はバイト単位のサイズとして扱われます。</p> <p>デフォルト値 : なし</p> <p>--HeuristicAnalysis <On/Off> - スキャン中のヒューリスティック解析を有効または無効にします。</p> <p>デフォルト値 : On</p> <p>--Cure <Yes/No> - 脅威が検出された際に修復を試みる動作を有効または無効にします。</p> <p>値にNoが指定された場合、検出された脅威に関する通知のみが表示されます。</p> <p>デフォルト値 : No</p> <p>--ListCleanItem - スキャンされたコンテナ内で見つかったクリーンな(感染していない)ファイルのリストの出力を有効にします。</p> <p>--ShellTrace - ファイルをスキャンする際の、追加のデバッグ情報の表示を有効にします。</p> <p>--Output <path to file> - コマンドの出力を指定されたファイルに複製します。</p>
remotescan <host> <path>	<p>機能 : <i>SSH</i>または <i>Telnet</i>を使用して接続することにより、指定されたリモートホスト上の指定されたファイルまたはディレクトリのスキャンを開始します。</p> <div data-bbox="608 1207 1449 1765" style="background-color: #fff9c4; padding: 10px;"><p> リモートスキャンで検出された脅威は駆除されず、threatsコマンドで表示される、検出された脅威のリストには含まれないということに注意してください(下記参照)。</p><hr/><p>この機能はリモートホストの悪意のあるファイルや疑わしいファイルの検出にのみ使用できます。リモートホストで検出された脅威を排除するには、このホストから直接提供される管理ツールを使用する必要があります。たとえば、ルーターの場合、セットトップボックスおよびその他のスマートデバイス、つまりファームウェア更新のためのメカニズムを使用することができます。コンピューティングマシンの場合、それらのマシン(オプションとして、リモートターミナルモードを使用)およびそれらのファイルシステムのそれぞれの操作(ファイルの削除または移動など)に接続するか、それらにインストールされたアンチウイルスソフトウェアを実行して行うことができます。</p></div> <p>引数</p> <ul style="list-style-type: none">• <host> - リモートホストのIPアドレスまたはドメイン名です。• <path> - スキャンするファイルまたはディレクトリへのパスです(パスは絶対パスでなければなりません)。



コマンド	説明
	<p>オプション</p> <p><code>-m [--Method] <SSH/Telnet></code> - リモートホスト接続方法(プロトコル)です。</p> <p>方法が指定されていない場合は、SSHが使用されます。</p> <p><code>-l [--Login] <name></code> - 選択されたプロトコル経由でリモートホストでの承認に使用されるログインID(ユーザー名)です。</p> <p>ユーザー名が指定されていない場合、コマンドを起動したユーザー名を用いてリモートホストに接続しようとしています。</p> <p><code>-i [--Identity] <path to file></code> - 選択されたプロトコル経由で指定されたユーザーの認証に使用されるプライベートキーが含まれるファイルへのパスです。</p> <p><code>-p [--Port] <number></code> - 選択されたプロトコル経由で接続するリモートホストのポート番号です。</p> <p>デフォルト値: 選択したプロトコル用のデフォルトポート (SSHでは22、Telnetでは23)</p> <p><code>--ForceInteractive</code> - SSHインタラクティブセッションを使用します (<i>SSH</i>接続の場合のみ)。</p> <p>オプション機能です。</p> <p><code>--TransferListenAddress <address></code> - リモートデバイスからスキャン用に送信されるファイルを受信するためにリッスンされるアドレスです。</p> <p>オプション機能です。指定されなかった場合、任意のアドレスが使用されます。</p> <p><code>--TransferListenPort <port></code> - リモートデバイスからスキャン用に送信されるファイルを受信するためにリッスンされるポートです。</p> <p>オプション機能です。指定されなかった場合、任意のポートが使用されます。</p> <p><code>--TransferExternalAddress <address></code> - スキャン用にファイルを送信するためにリモートデバイスに指定されるアドレスです。</p> <p>オプション機能です。指定されなかった場合、"<code>--TransferListenAddress</code>"の値、またはすでに確立されているセッションの送信アドレスが使用されます。</p> <p><code>--TransferExternalPort <port></code> - スキャン用にファイルを送信するためにリモートデバイスに指定されるポートです。</p> <p>オプション機能です。指定されなかった場合、自動的に決定されたポートが使用されます。</p> <p><code>--Password <password></code> - 選択されたプロトコルを介してユーザー認証に使用されるパスワードです。</p> <p>パスワードはプレーンテキストとして転送されることに注意してください。</p> <p><code>--Exclude <path></code> - スキャンの対象から除外するパスです。パスにはファイルマスクを含むことができます (ワイルドカード「?」と「*」、シンボルクラス「[]」、「[!]」、「[^]」を使用することができます)。パス(ファイルマスクを含むパスを含む)は絶対パスである必要があります。</p> <p>任意オプション、複数回設定できます。</p> <p><code>--Report <type></code> - スキャンレポートのタイプを指定します。</p>



コマンド	説明
	<p>使用可能な値:</p> <ul style="list-style-type: none">• BRIEF - 短いレポート• DEBUG - 詳細なレポート• JSON - JSON形式のシリアル化されたレポート <p>デフォルト値: BRIEF</p> <p><code>--ScanTimeout <number></code> - 1つのファイルをスキャンする際のタイムアウトをミリ秒で指定します。</p> <p>値に0が指定された場合、スキャンにかかる時間は制限されません。</p> <p>デフォルト値: 0</p> <p><code>--PackerMaxLevel <number></code> - 圧縮されたオブジェクトをスキャンする際のネスティングレベルの上限を指定します。圧縮されたオブジェクトは、特別なソフトウェア (UPX、PELock、PECompact、Petite、ASPack、Morphineなど) で圧縮された実行コードです。そのようなオブジェクトには、圧縮されたオブジェクトなども含む他の圧縮されたオブジェクトが含まれる場合があります。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他の圧縮されたオブジェクト内の圧縮されたオブジェクトはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値: 8</p> <p><code>--ArchiveMaxLevel <number></code> - 他のアーカイブが含まれる可能性のあるアーカイブ (zip、rarなど) をスキャンするときの最大ネスティングレベルを設定します (これらのアーカイブには他のアーカイブなどが含まれる場合もあります)。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他のアーカイブ内のアーカイブはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値: 8</p> <p><code>--MailMaxLevel <number></code> - 他のファイルが含まれる可能性のあるメーラーのファイル (pst、tbbなど) をスキャンするときの最大ネスティングレベルを設定します (これらのファイルには他のファイルなどが含まれる場合もあります)。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他のオブジェクト内のオブジェクトはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値: 8</p> <p><code>--ContainerMaxLevel <number></code> - 他のオブジェクトが含まれる他のタイプのオブジェクト (HTMLページ、jarファイルなど) をスキャンするときの最大ネスティングレベルを設定します。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他のオブジェクト内のオブジェクトはスキャンされません。</p> <p>値に0が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。</p> <p>デフォルト値: 8</p> <p><code>--MaxCompressionRatio <ratio></code> - スキャンされるオブジェクトの最大圧縮率を指定します。</p> <p>値は2以上にする必要があります。</p>



コマンド	説明
	<p>デフォルト値 : 3000</p> <p>--MaxSizeToExtract <size> - アーカイブに含まれるファイルの最大サイズを指定します。このパラメータの値よりサイズが大きいファイルは、スキャン時にスキップされます。デフォルトでは、アーカイブ内のファイルのサイズ制限はありません。サイズは、サフィックス(b, kb, mb, gb)を付けた数値で指定します。サフィックスが指定されていない場合、値はバイト単位のサイズとして扱われます。</p> <p>デフォルト値 : なし</p> <p>--HeuristicAnalysis <On/Off> - スキャン中のヒューリスティック解析を有効または無効にします。</p> <p>デフォルト値 : On</p>

3.2. 更新および集中管理モードでの動作を管理するコマンド


更新および集中管理モードでの動作を管理するコマンドには、以下のものがあります。

コマンド	説明
update	<p>機能 : Dr.Web MeshDを介して、Doctor Webの更新サーバーまたはローカルクラウドから、アンチウイルスコンポーネント(ディストリビューションによって、ウイルスデータベース、スキャンエンジンなど)の更新を開始し、更新プロセスがすでに実行されている場合はそれを終了するか、または更新ファイルの最新の更新を以前のバージョンへロールバックします。</p> <div style="border: 1px solid #ccc; background-color: #e6f2e6; padding: 10px; margin: 10px 0;">  Dr.Web for UNIX Internet Gatewaysが集中管理サーバーに接続されている場合、このコマンドは効力を持ちません。 </div> <p>引数 : なし</p> <p>オプション</p> <p>-l [--local-cloud] - Dr.Web for UNIX Internet Gatewaysに接続されたローカルクラウドを使用して更新をダウンロードします。このオプションが指定されていない場合、更新はDoctor Web更新サーバーからダウンロードされます(デフォルトの動作)。</p> <p>--From <path> - 指定されたディレクトリからオフラインで更新を適用します。</p> <p>--Path <path> - オフラインで更新するファイルを指定されたディレクトリに保存します。このディレクトリにすでにファイルがある場合は、それらが更新されません。</p> <p>--Rollback - 最後の更新をロールバックし、更新されたファイルの以前のバージョンを復元します。</p> <p>--Stop - 実行中の更新プロセスを終了します。</p>
esconnect <server>[: <port>]	<p>機能 : 指定された集中管理サーバー(Dr.Web Enterprise Serverなど)にDr.Web for UNIX Internet Gatewaysを接続します。動作モードの詳細については、動作モードを参照してください。</p>



コマンド	説明
	<p>引数</p> <ul style="list-style-type: none">• <code><server></code> - 集中管理サーバーが動作しているホストのIPアドレスまたはホスト名です。この引数は必須です。• <code><port></code> - 集中管理サーバーによって使用されるポート番号です。この引数は任意であり、集中管理サーバーが標準以外のポートを使用する場合にのみ指定する必要があります。 <p>オプション</p> <p><code>--Certificate <path></code> - 接続する集中管理サーバーの証明書ファイルへのパスです。</p> <p><code>--Login <ID></code> - 集中管理サーバーへの接続に使用されるログインID(ワークステーションID)です。</p> <p><code>--Password <password></code> - 集中管理サーバーへの接続用パスワードです。</p> <p><code>--Group <ID></code> - ワークステーションが接続時に追加されるグループのIDです。</p> <p><code>--Rate <ID></code> - ワークステーションが集中管理サーバーグループの1つに含まれている場合に、そのワークステーションに適用される課金プラングループのIDです(<code>--Group</code>オプションと一緒にのみ指定できます)。</p> <p><code>--Compress <On/Off></code> - 送信されたデータの強制的な圧縮を有効(On)または無効(Off)にします。指定しない場合、圧縮の使用はサーバーによって決定されます。</p> <p><code>--Encrypt <On/Off></code> - 送信されたデータの強制的な暗号化を有効(On)または無効(Off)にします。指定しない場合、暗号化の使用はサーバーによって決定されます。</p> <p><code>--Newbie</code> - 「新規端末」として接続します(サーバーで新しいアカウントを取得します)。</p> <div data-bbox="609 1294 1449 1442" style="border: 1px solid #ccc; background-color: #e6f2e6; padding: 10px;"><p> このコマンドは、<code>drweb-ctl</code>を<code>root</code>権限で実行する必要があります。必要に応じて、<code>su</code>または<code>sudo</code>コマンドを使用してください。</p></div>
esdisconnect	<p>機能 : Dr.Web for UNIX Internet Gatewaysを集中管理サーバーから切断し、その動作をスタンドアロンモードに切り替えます。</p> <div data-bbox="609 1572 1449 1720" style="border: 1px solid #ccc; background-color: #e6f2e6; padding: 10px;"><p> Dr.Web for UNIX Internet Gatewaysがすでにスタンドアロンモードで動作している場合、このコマンドは効力を持ちません。</p></div> <p>引数 : なし</p> <p>オプション : なし</p>



コマンド	説明
	 このコマンドは、 <code>drweb-ctl</code> を <code>root</code> 権限で実行する必要があります。必要に応じて、 <code>su</code> または <code>sudo</code> コマンドを使用してください。

3.3. 設定を管理するコマンド

設定を管理するコマンドには以下のものがあります。

コマンド	説明
<code>cfset</code> <code><section> . <parameter></code> <code><value></code>	<p>機能 : Dr.Web for UNIX Internet Gatewaysの現在の設定で、指定されたパラメータのアクティブな値を変更します。</p> <p>引数</p> <ul style="list-style-type: none">• <code><section></code> - パラメータのある設定ファイルのセクション名です。この引数は必須です。• <code><parameter></code> - パラメータの名前です。この引数は必須です。• <code><value></code> - 新しいパラメータ値です。この引数は必須です。 <div style="border: 1px solid #ccc; padding: 10px; background-color: #f0f8e0;"><p> パラメータ値を指定するには、<code><section> . <parameter> <value></code>という形式を使用します。代入記号「=」はここでは使用しません。</p><p>複数のパラメータ値を指定する場合は、追加するパラメータ値の数だけ<code>cfset</code>コマンドの呼び出しを繰り返す必要があります。パラメータ値のリストに新しい値を追加するには、<code>-a</code>オプションを使用します(以下を参照)。文字列"<code><value 1></code>, <code><value 2></code>"が<code><parameter></code>の1つの値と見なされてしまうため、文字列<code><parameter> <value 1></code>, <code><value 2></code>を引数として指定することはできません。</p><p>設定ファイルに関する詳細は、付録D. Dr.Web for UNIX Internet Gateways設定ファイルのセクションを参照してください。また、<code>man 5 drweb.ini</code>によって表示されるドキュメントページも参照してください。</p></div> <p>オプション</p> <ul style="list-style-type: none">-a [<code>--Add</code>] - 現在のパラメータ値を置き換えず、指定された値をリストに追加します(リストとして指定された複数の値を持つことのできるパラメータに対してのみ使用可能)。このオプションは、タグを付けたパラメータの新しいグループを追加する場合にも使用してください。-e [<code>--Erase</code>] - 現在のパラメータ値を置き換えず、指定された値をリストから削除します(リストとして指定された複数の値を持つことのできるパラメータに対してのみ使用可能)。-r [<code>--Reset</code>] - パラメータ値をデフォルトにリセットします。その際、コマンド内で<code><value></code>は必要なく、指定された場合は無視されます。



コマンド	説明
	<p>オプションは必須ではありません。指定されなかった場合は、現在のパラメータ値（パラメータに複数の値がある場合は値の全リスト）が指定された値に置き換えられます。</p> <p>Dr.Web ClamDの接続ポイントの個々のパラメータを記述するセクションでは、<code>-r</code>オプションを使用すると、個々の設定セクションのパラメータ値が、該当するコンポーネントの設定にある親パラメータの値に置き換えられます。</p> <p>Dr.Web ClamDの新しい接続ポイント <code><point></code> を追加する必要がある場合は、次のコマンドを使用します。</p> <pre>cfset ClamD.Endpoint.<point> -a</pre> <p>例: <code>cfset ClamD.Endpoint.point1 -a</code></p> <div data-bbox="619 689 1449 840" style="border: 1px solid #ccc; background-color: #e6f2e6; padding: 10px;"><p> このコマンドは、<code>drweb-ctl</code>をroot権限で実行する必要があります。必要に応じて、<code>su</code>または<code>sudo</code>コマンドを使用してください。</p></div>
<pre>cfshow [<section>[. <parameter>]</pre>	<p>機能 : Dr.Web for UNIX Internet Gatewaysの現在の設定のパラメータを表示します。</p> <p>パラメータを表示するコマンドは <code><section>.<parameter> = <value></code> のように指定します。インストールされていないコンポーネントのセクションとパラメータは表示されません。</p> <p>引数</p> <ul style="list-style-type: none">• <code><section></code> - 表示するパラメータのある設定ファイルのセクション名です。この引数は任意です。指定されなかった場合、すべての設定ファイルセクションのパラメータが表示されます。• <code><parameter></code> - 表示するパラメータの名前です。この引数は任意です。指定されなかった場合、セクションのすべてのパラメータが表示されます。それ以外の場合は、このパラメータのみが表示されます。セクション名なしにパラメータが指定された場合、すべての設定ファイルセクションにある、その名前を持つすべてのパラメータが表示されます。 <p>オプション</p> <p><code>--Uncut</code> - すべての設定パラメータを表示します（現在インストールされているコンポーネントのセットによって使用されているもの以外も含む）。このオプションが指定されていない場合、インストールされたコンポーネントの設定に使用されているパラメータのみが出力されます。</p> <p><code>--Changed</code> - デフォルトの値と異なる値を持つパラメータのみを表示します。</p> <p><code>--Ini</code> - パラメータ値をINIファイルフォーマットで表示します。まず角括弧内でセクション名が指定され、次に <code><parameter> = <value></code> ペアでセクションパラメータが表示されます（1行につき1ペア）。</p> <p><code>--Value</code> - 指定されたパラメータの値のみを表示します（この場合、<code><parameter></code>引数は必須です）。</p>
<pre>reload</pre>	<p>機能 : Dr.Web ConfigD設定デーモンにSIGHUPシグナルを送信します。</p> <p>このシグナルを受信すると、Dr.Web ConfigD設定デーモンは設定を再読み込みし、そこに加えられた変更をDr.Web for UNIX Internet Gatewaysのコンポーネントに送信します。次に、Dr.Web for UNIX Internet Gatewaysログを再度</p>



コマンド	説明
	<p>開き、ウイルスデータベースを使用するコンポーネント(スキャンエンジンを含む)を再起動させ、異常終了したコンポーネントの再起動を試みます。</p> <p>引数: なし</p> <p>オプション: なし</p>

3.4. 検出された脅威および隔離を管理するコマンド

検出された脅威および隔離を管理するコマンドには以下のものがあります。

コマンド	説明
<code>threats</code> [<code><action></code> <code><object></code>]	<p>機能: 検出された脅威のうち、識別子で選択されたものに対して、指定されたアクションを適用します。アクションの種類はコマンドオプションによって指定します。</p> <p>アクションが指定されていない場合、検出されたが駆除されていない脅威に関する情報を表示します。脅威に関する情報は、オプションの <code>--Format</code> 引数で指定されたフォーマットに従って表示されます。<code>--Format</code> 引数が指定されていない場合は、各脅威に関する次の情報が表示されます。</p> <ul style="list-style-type: none">• 脅威に対して割り当てられた識別子(順序数)• 感染したファイルへのフルパス• 脅威に関する情報(脅威の名前、Doctor Webの分類による脅威の種類)• ファイルに関する情報(サイズ、ファイル所有者のユーザー名、最後に変更された時間)• 脅威に対して適用された操作の履歴(検出、適用されたアクションなど) <p>引数: なし</p> <p>オプション</p> <p><code>--Format</code> "<code><format string></code>" - 脅威に関する情報を指定されたフォーマットで表示します。フォーマット文字列の説明は 以下のとおりです。</p> <p>このオプションがアクションオプションと一緒に指定されている場合は無視されます。</p> <p><code>-f</code> [<code>--Follow</code>] - 新しい脅威に関する新しいメッセージを待ち、それらを受け取り次第、表示します(CTRL+Cで待機を中断します)。</p> <p>このオプションがアクションオプションと一緒に指定されている場合は無視されます。</p> <p><code>--Directory</code> <code><list of directories></code> - <code><list of directories></code>で指定したディレクトリ内のファイルで検出された脅威のみを表示します。</p> <p>このオプションが以下のオプションと一緒に適用された場合は無視されます。</p> <p><code>--Cure</code> <code><threat list></code> - 指定された脅威の修復を試みます(脅威の識別子をコンマ区切りで指定)。</p> <p><code>--Quarantine</code> <code><threat list></code> - 指定された脅威を 隔離に移します(脅威の識別子をコンマ区切りで指定)。</p>



コマンド	説明
	<p>--Delete <threat list> - 指定された脅威を削除します (脅威の識別子をコンマ区切りで指定)。</p> <p>--Ignore <threat list> - 指定された脅威を無視します (脅威の識別子をコンマ区切りで指定)。</p> <p>検出されたすべての脅威に対してアクションを適用する必要がある場合は、<threat list>の代わりにAllを指定します。例：</p> <pre data-bbox="576 501 1442 573">\$ drweb-ctl threats --Quarantine All</pre> <p>この例では、検出された悪意のあるオブジェクトすべてを隔離に移します。</p>
quarantine [<action> <object>]	<p>機能： 隔離内の指定されたオブジェクトに対してアクションを適用します。</p> <p>アクションが指定されなかった場合、隔離されたオブジェクトに関する情報とそのIDが、隔離に移された元のファイルに関する簡単な情報と一緒に表示されます。隔離されたオブジェクトに関する情報は、オプションの--Format引数で指定されたフォーマットに従って表示されます。--Format引数が指定されていない場合は、隔離された各オブジェクトについて次の情報が表示されます。</p> <ul data-bbox="576 904 1442 1144" style="list-style-type: none">• 隔離されたオブジェクトに対して割り当てられた識別子• 隔離に移される前の、元のファイルへのパス• ファイルが隔離に移された日付• ファイルに関する情報 (サイズ、ファイル所有者のユーザー名、最後に変更された時間)• 脅威に関する情報 (脅威の名前、Doctor Webの分類による脅威の種類) <p>引数：なし</p> <p>オプション</p> <p>-a [--Autonomous] - 指定された隔離コマンドを実行するために Dr.Web File Checker ファイルスキャンコンポーネントの個別のインスタンスを開始し、完了後にそれを終了します。</p> <p>このオプションは以下のオプションと一緒に適用できます。</p> <p>--Format " <format string>" - 隔離されたオブジェクトに関する情報を指定されたフォーマットで表示します。フォーマット文字列の説明は 以下のとおりです。</p> <p>このオプションがアクションオプションと一緒に指定されている場合は無視されます。</p> <p>-f [--Follow] - 新しい脅威に関する新しいメッセージを待ち、それらを受け取り次第、表示します (CTRL+Cで待機を中断します)。</p> <p>このオプションがアクションオプションと一緒に指定されている場合は無視されます。</p> <p>--Discovery [<list of directories>] - 指定されたディレクトリのリストで 隔離ディレクトリを検索し、脅威を検出すると、統合された隔離に追加します。<list of directories>が指定されていない場合は、ファイルシステムの共通の場所 (ボリュームマウントポイントとユーザーホームディレクトリ)にある隔離ディレクトリを検索します。</p>



コマンド	説明
	<p>このオプションは <code>-a(--Autonomous)</code> オプション(上記を参照)だけでなく、下記に一覧で示されている任意のオプションおよびアクションとともに指定できます。さらに、自律コピーとして <code>quarantine</code> コマンドを起動すると (<code>-a(--Autonomous)</code> オプションを指定して、<code>--Discovery</code> オプションは指定しない場合)、次の呼び出しと同じになります。</p> <pre data-bbox="612 427 1441 499">quarantine --Autonomous --Discovery</pre> <p><code>--Delete <object></code> - 指定されたオブジェクトを隔離から削除します。 オブジェクトは隔離から永久に削除されることに注意してください。この操作は元に戻せません。</p> <p><code>--Cure <object></code> - 隔離内の指定されたオブジェクトの修復を試みます。 オブジェクトが修復された場合であっても、それは隔離内に残ります。修復されたオブジェクトを隔離から復元するには <code>--Restore</code> オプションを使用します。</p> <p><code>--Restore <object></code> - 指定されたオブジェクトを隔離から元の場所に復元します。 このコマンドでは、<code>drweb-ctl</code> を root 権限で起動する必要がある場合があります。感染していても隔離からファイルを復元できます。</p> <p><code>--TargetPath <path></code> - オブジェクトを隔離から指定された場所に復元します。指定された名前を持つファイルとして復元するか (<code><path></code> がファイルへのパスであった場合)、またはただ単に指定されたディレクトリに復元します (<code><path></code> がディレクトリへのパスであった場合)。パスは絶対パスでも相対パスでも構いません(現在のディレクトリを参照)。 このオプションは、<code>--Restore</code> オプションとの組み合わせでのみ使用できます。</p> <p><code><object></code> は隔離内のオブジェクトの識別子を指定します。隔離されたすべてのオブジェクトに対してアクションを適用する場合は、<code><object></code> の代わりに <code>All</code> を指定してください。例：</p> <pre data-bbox="571 1317 1441 1422">\$ drweb-ctl quarantine --Restore All --TargetPath test</pre> <p>すべての隔離されたオブジェクトを、<code>drweb-ctl</code> コマンドが起動されたカレントディレクトリにある <code>test</code> サブディレクトリに復元します。</p> <p><code>--Restore All</code> では、追加のオプション <code>--TargetPath</code> (指定された場合) にはファイルへのパスではなくディレクトリへのパスを指定する必要があります。</p>

脅威および隔離コマンド用のフォーマット出力



出力フォーマットは、オプションの`--Format`引数として指定されたフォーマット文字列を使用して定義されません。フォーマット文字列は引用符で囲んで指定する必要があります。フォーマット文字列には、特定の情報として表示される特殊なマーカーだけでなく、一般的な記号(「そのまま」で表示されるもの)を含めることができます。以下のマーカーを使用することができます。

1. threatsとquarantineコマンドに共通:

マーカー	説明
<code>%{n}</code>	新しい文字列
<code>%{t}</code>	集計
<code>%{threat_name}</code>	Doctor Webの分類に従って検出された脅威(ウイルス)の名前
<code>%{threat_type}</code>	Doctor Webの分類に従った脅威の種類(「既知のウイルス」など)
<code>%{size}</code>	元のファイルサイズ
<code>%{origin}</code>	パスを含む元のファイルのフルネーム
<code>%{path}</code>	<code>%{origin}</code> の同義語
<code>%{ctime}</code>	元のファイルが変更された日時("%Y-%b-%d %H:%M:%S"フォーマット、例: "2018-Jul-20 15:58:01")
<code>%{timestamp}</code>	<code>%{ctime}</code> と似ているが、UNIXのタイムスタンプフォーマット
<code>%{owner}</code>	元のファイル所有者のユーザー名
<code>%{rowner}</code>	元のファイルのリモートユーザー所有者(該当しない場合や値が不明な場合は?と置き換えられます)

2. threatsコマンドに固有:

マーカー	説明
<code>%{hid}</code>	脅威に関連付けられているイベントの履歴にある脅威レコードのID
<code>%{tid}</code>	脅威のID
<code>%{htime}</code>	脅威に関連したイベントの日時
<code>%{app}</code>	脅威を処理したDr.Web for UNIX Internet GatewaysコンポーネントのID
<code>%{event}</code>	脅威に関連する最新イベント: <ul style="list-style-type: none">• FOUND - 脅威が検出されました。• Cure - 脅威は修復されました。• Quarantine - 脅威のあるファイルが隔離に移されました。• Delete - 脅威のあるファイルが削除されました。• Ignore - 脅威は無視されました。• RECAPTURED - 他のコンポーネントによって脅威が再度検出されました。



マーカー	説明
<code>%{err}</code>	エラーメッセージテキスト(エラーが空の文字列に置き換えられない場合)

3. quarantineコマンドに固有:

マーカー	説明
<code>%{qid}</code>	隔離されたオブジェクトのID
<code>%{qtime}</code>	オブジェクトを隔離に移動した日時
<code>%{curetime}</code>	隔離に移されたオブジェクトの修復を試みた日時(該当しない場合または値が不明の場合は?に置き換えられます)
<code>%{cureres}</code>	隔離されたオブジェクトの修復を試みた結果: <ul style="list-style-type: none"> • <code>cured</code> - 脅威は修復されています。 • <code>not cured</code> - 脅威は修復されていないか、修復が試みられていません。

例

```
$ drweb-ctl quarantine --Format "{%{n} %{origin}: %{threat_name} - %{qtime}%{n}}"
```

このコマンドは、次のタイプのレコードとして隔離内容を表示します。

```
{
  <path to file>: <threat name> - <date of moving to quarantine>
}
...
```

3.5.情報に関するコマンド

情報に関するコマンドには以下のものがあります。

コマンド	説明
<code>appinfo</code>	<p>機能: アクティブな Dr.Web for UNIX Internet Gatewaysコンポーネントに関する情報を出力します。</p> <p>現在実行中の各コンポーネントに関する以下の情報が表示されます。</p> <ul style="list-style-type: none"> • 内部で使用される名前 • プロセス識別子 GNU/Linux(PID) • 状態(実行中、停止など) • コンポーネントの動作がエラーによって終了した場合、エラーコード • 追加情報(任意) <p>設定デーモン(<code>drweb-configd</code>)については、以下の追加情報が表示されます。</p> <ul style="list-style-type: none"> • インストールされたコンポーネントのリスト - <i>Installed</i>



コマンド	説明
	<ul style="list-style-type: none">設定デーモンによって起動する必要のあるコンポーネントのリスト - <i>Should run</i> <p>引数 : なし</p> <p>オプション</p> <p>-f [--Follow] - モジュールのステータス変更に関する新しい情報を待ち、それらを受け取り次第メッセージを表示します (CTRL+Cで待機を中断します)。</p>
baseinfo	<p>機能 : スキャンエンジンの現在のバージョン、およびウイルスデータベースのステータスに関する情報を表示します。</p> <p>以下の情報が表示されます。</p> <ul style="list-style-type: none">スキャンエンジンのバージョン現在使用されているウイルスデータベースがリリースされた日時(ウイルスデータベース内の) 使用可能なウイルスレコードの数ウイルスデータベースおよびスキャンエンジンが最後に更新された時間スケジュールされている次の自動更新の時間 <p>引数 : なし</p> <p>オプション</p> <p>-l [--List] - ダウンロードされたウイルスデータベースのファイルと各ファイルのウイルスレコード数の全リストを表示します。</p>
certificate	<p>機能 : Dr.Web for UNIX Internet Gatewaysによって使用される、信頼できるDr.Web証明書のコンテンツを表示します。証明書を<cert_name>.pemファイルに保存するには、以下のコマンドを使用できます。</p> <pre data-bbox="568 1256 1437 1335">\$ drweb-ctl certificate > <cert_name>.pem</pre> <p>引数 : なし</p> <p>オプション : なし</p>
events	<p>機能 : Dr.Web for UNIX Internet Gatewaysイベントを表示します。その他、このコマンドを使用してイベントを管理 (既読としてマーク、削除) できます。</p> <p>引数 : なし</p> <p>オプション</p> <p>--Report <type> - イベントレポートのタイプを指定します。</p> <p>使用可能な値 :</p> <ul style="list-style-type: none">BRIEF - 短いレポートDEBUG - 詳細なレポートJSON - JSON形式のシリアル化されたレポート <p>-f [--Follow] - 新しいイベントを待ち、発生時にそれらを表示します (CTRL+Cでスタンバイを中断します)。</p>



コマンド	説明
	<p>-s [--Since] <date, time> - 指定されたタイムスタンプの前に発生したイベントを表示します (<date, time>は YYYY-MM-DD hh:mm:ss のフォーマットで指定します)。</p> <p>-u [--Until] <date, time> - 指定されたタイムスタンプよりも前に発生したイベントを表示します (<date, time>は YYYY-MM-DD hh:mm:ss のフォーマットで指定します)。</p> <p>-t [--Types] <type list> - 指定されたタイプのイベントのみを表示します (コンマで区切られます)。</p> <p>次のイベントタイプを使用できます。</p> <ul style="list-style-type: none">• Mail - メール内で脅威を検出したことを示します。• UnexpectedAppTermination - コンポーネントの予期しないシャットダウン。 <p>すべてのタイプのイベントを表示するには、Allを使用します。</p> <p>--ShowSeen - 既読イベントも表示します。</p> <p>--Show <list of events> - リストアップされたイベントを表示します (イベント識別子はコンマで区切られます)。</p> <p>--Delete <list of events> - リストアップされたイベントを削除します (イベント識別子はコンマで区切られます)。</p> <p>--MarkAsSeen <list of events> - リストアップされたイベントを既読としてマークします (イベント識別子はコンマで区切られます)。</p> <p>すべてのイベントを「既読」としてマークする場合や削除する場合は、<events list>ではなくAllを指定します。例：</p> <pre data-bbox="571 1137 1439 1211">\$ drweb-ctl events --MarkAsSeen All</pre> <p>このコマンドはすべてのイベントを「既読」としてマークします。</p>
report <type>	<p>機能 : Dr.Web for UNIX Internet Gatewaysのイベントに関するレポートをHTML形式で作成します (ページ本文は指定したファイルに出力されます)。</p> <p>引数</p> <p><type> - レポートを作成するイベントのタイプです (タイプを1つ指定します)。可能な値については、上記 events コマンドの --Types オプションの説明を参照してください。この引数は必須です。</p> <p>オプション</p> <p>-o [--Output] <path to file> - 指定したファイルにレポートを保存します。このオプションは必須です。</p> <p>-s [--Since] <date, time> - 指定されたタイムスタンプよりも後に発生したイベントのレポートを作成します (<date, time>は YYYY-MM-DD hh:mm:ss のフォーマットで指定します)。</p> <p>-u [--Until] <date, time> - 指定されたタイムスタンプよりも前に発生したイベントのレポートを作成します (<date, time>は YYYY-MM-DD hh:mm:ss のフォーマットで指定します)。</p> <p>--TemplateDir <path to directory> - HTMLレポートテンプレートを含むディレクトリへのパスです。</p>



コマンド	説明
	<p>-s、-u、--TemplateDirは必須のオプションではありません。</p> <pre data-bbox="571 315 1437 387">\$ drweb-ctl report Mail -o report.html</pre> <p>たとえば、上記のコマンドは、メールメッセージでのすべての脅威検出イベントに関するレポートをデフォルトのテンプレートで生成し、結果をカレントディレクトリのreport.htmlファイルに保存します。</p>
license	<p>機能：現在有効なライセンスに関する情報を表示するか、デモバージョンのライセンスを取得するか、またはすでに登録されているライセンス(すでにWebサイト上で登録されているものなど)のキーファイルを取得します。</p> <p>オプションが指定されていない場合は以下の情報が表示されます(スタンドアロンモードのライセンスを使用している場合)。</p> <ul style="list-style-type: none">• ライセンス番号• ライセンスの有効期間が満了する日時 <p>集中管理サーバーから受け取ったライセンスを使用している場合(集中管理モードまたはモバイルモードで製品を使用するため)、該当するメッセージが表示されます。</p> <p>引数：なし</p> <p>オプション</p> <p>--GetRegistered <serial number> - 新しいキーファイルの提供に関する条件に違反(ライセンスが集中管理サーバーによって管理される場合に製品を集中管理モードで使用していないなど)していない場合、指定されたシリアル番号に対するライセンスキーファイルを取得します。</p> <p>シリアル番号が試用期間用のものではない場合、まず Doctor WebのWebサイトでそれを登録する必要があります。</p> <p>--Proxy http://<username>:<password>@<server address>:<port number> - プロキシサーバー経由でライセンスキーファイルを取得します(--GetRegisteredオプションとのみ使用できます)。</p> <p>Dr.Web製品のライセンスに関する詳細については、ライセンスのセクションを参照してください。</p> <div data-bbox="608 1473 1449 1599"> シリアル番号を登録するにはインターネット接続が必要です。</div>
log	<p>機能：Dr.Web for UNIX Internet Gatewaysの最新のログレコードをコンソール画面に(stdoutスレッドで)表示します(tailコマンドと同様)。</p> <p>引数：なし</p> <p>オプション</p> <p>-s [--Size] <number> - 画面に表示される最後のログレコードの数。</p> <p>-c [--Components] <components list> - そのレコードを表示する必要があるコンポーネントのIDのリストです。IDはコンマで区切って指定します。この引</p>



コマンド	説明
	<p>数が指定されていない場合、あらゆるコンポーネントによってログに記録されたすべてのレコードが表示されます。</p> <p>インストールされているコンポーネントの実際のID(ログに表示される内部コンポーネント名など)は、<code>appinfo</code>コマンドを使用して指定できます(上記を参照)。</p> <p><code>-f [--Follow]</code> - ログ内の新しいメッセージを待ち、それらを受け取り次第メッセージを表示します(CTRL+Cキーを押して待機を中断します)。</p>
<code>stat</code>	<p>機能 : ファイルを処理するコンポーネント、またはネットワークデータのスキャンエージェント Dr.Web Network Checker の動作に関する統計情報を出力します(CTRL+CまたはQを押すと統計情報の表示を中断します)。</p> <p>出力される統計情報には以下が含まれます。</p> <ul style="list-style-type: none">• スキャンを開始したコンポーネントの名前• コンポーネントのPID• 最後の1分間、5分間、15分間に処理された1秒あたりの平均ファイル数• スキャンされたファイルキャッシュの使用率• 1秒あたりのスキャンエラーの平均数 <p>分散スキャンエージェントについては、以下の情報が出力されます。</p> <ul style="list-style-type: none">• スキャンを開始したローカルクライアントのリスト• スキャンのためにファイルを受信したリモートホストのリスト• スキャンのためにファイルを送信したリモートホストのリスト <p>分散スキャンエージェントのローカルクライアントについてはPIDと名前が、リモートクライアントについてはホストのアドレスとポートが出力されます。</p> <p>ローカルとリモートの両方のクライアントについて、次の情報が出力されます。</p> <ul style="list-style-type: none">• 1秒間にスキャンされたファイルの平均数• 1秒あたりの送信および受信バイトの平均数• 1秒あたりのエラーの平均数 <p>引数 : なし</p> <p>オプション</p> <p><code>-n [--netcheck]</code> - ネットワークデータのスキャンエージェントの動作に関する統計情報を出力します。</p>

使用例

このセクションでは、Dr.Web Ctl(`drweb-ctl`)ユーティリティの使用例を示します。

- オブジェクトのスキャン:
 - [シンプルなスキャンのコマンド](#)
 - [条件によって選択されたファイルのスキャン](#)
 - [追加のオブジェクトのスキャン](#)
- [設定の管理](#)
- [脅威の管理](#)



- [自律コピーモードでの動作例](#)

1. オブジェクトのスキャン

1.1. シンプルなスキャンのコマンド

1. デフォルトのパラメータで/homeディレクトリのスキャンを実行する:

```
$ drweb-ctl scan /home
```

2. `daily_scan`ファイルに含まれているパスをスキャンする(1行につき1つのパス):

```
$ drweb-ctl scan --stdin < daily_scan
```

3. `sda`ドライブ上のブートレコードのスキャンを実行する:

```
$ drweb-ctl bootscan /dev/sda
```

4. 実行中のプロセスのスキャンを実行する:

```
$ drweb-ctl procsan
```

1.2. 条件によって選択されたファイルのスキャン

以下は、スキャンの対象となるファイルの選択と、`find`ユーティリティの操作結果の使用例です。取得したファイルのリストは、`--stdin`または`--stdin0`パラメータを指定して`drweb-ctl scan`コマンドに送信されません。

1. `find`ユーティリティによって返されたリストに含まれ、NUL(`\0`)記号で区切られたファイルのスキャンする:

```
$ find -print0 | drweb-ctl scan --stdin0
```

2. ファイルシステムの1つのパーティション上の、ルートディレクトリから始まり、すべてのディレクトリ内にあるすべてのファイルのスキャンする:

```
$ find / -xdev -type f | drweb-ctl scan --stdin
```

3. `/var/log/messages`および`/var/log/syslog`ファイルを除いて、ルートディレクトリから始まり、すべてのディレクトリ内にあるすべてのファイルのスキャンする:

```
$ find / -type f ! -path /var/log/messages ! -path /var/log/syslog |  
drweb-ctl scan --stdin
```

4. ルートディレクトリから始まり、すべてのディレクトリ内にある`root`ユーザーのすべてのファイルのスキャンする:

```
$ find / -type f -user root | drweb-ctl scan --stdin
```

5. ルートディレクトリから始まり、すべてのディレクトリ内にある`root`および`admin`ユーザーのファイルのスキャンする:

```
$ find / -type f \( -user root -o -user admin \) | drweb-ctl scan --stdin
```



6. ルートディレクトリから始まり、すべてのディレクトリ内にある、UIDが1000～1005の範囲内にあるユーザーのファイルをスキャンする:

```
$ find / -type f -uid +999 -uid -1006 | drweb-ctl scan --stdin
```

7. ルートディレクトリから始まり、ネスティングレベルが5以下のすべてのディレクトリ内にあるファイルをスキャンする:

```
$ find / -maxdepth 5 -type f | drweb-ctl scan --stdin
```

8. サブディレクトリ内のファイルを見逃して、ルートディレクトリ内にあるファイルをスキャンする:

```
$ find / -maxdepth 1 -type f | drweb-ctl scan --stdin
```

9. ルートディレクトリから始まり、すべてのディレクトリ内にあるファイルをすべてのシンボリックリンクをたどりながらスキャンする:

```
$ find -L / -type f | drweb-ctl scan --stdin
```

10. ルートディレクトリから始まり、すべてのディレクトリ内にあるファイルをシンボリックリンクをたどらずにスキャンする:

```
$ find -P / -type f | drweb-ctl scan --stdin
```

11. ルートディレクトリから始まり、すべてのディレクトリ内にある2017年5月1日以前に作成されたファイルをスキャンする:

```
$ find / -type f -newermt 2017-05-01 | drweb-ctl scan --stdin
```

1.3. 追加のオブジェクトのスキャン

1. リモートホスト192.168.0.1上の/tmpディレクトリ内にあるオブジェクトを、*user*ユーザーとしてパスワード*passwd*を使用してSSH経由でそれらに接続することでスキャンする:

```
$ drweb-ctl remotescan 192.168.0.1 /tmp --Login user --Password passwd
```

2. 設定の管理

1. 実行中のコンポーネントに関する情報を含む、現在のDr.Web for UNIX Internet Gatewaysパッケージに関する情報を表示する:

```
$ drweb-ctl appinfo
```

2. アクティブな設定の[Root]セクションからすべてのパラメータを出力する:

```
$ drweb-ctl cfshow Root
```

3. アクティブな設定の[LinuxSpider]セクション内でStartパラメータに「No」を設定する(これによりファイルシステムモニターSpIDer Guardが無効になります):

```
# drweb-ctl cfset LinuxSpider.Start No
```




このアクションを実行するにはスーパーユーザー権限が必要です。権限を昇格させるには、以下の例のようにsudoコマンドを使用できます。

```
$ sudo drweb-ctl cfset LinuxSpider.Start No
```

4. Dr.Web for UNIX Internet Gatewaysのアンチウイルスコンポーネントを強制的に更新する:

```
$ drweb-ctl update
```

5. Dr.Web for UNIX Internet Gatewaysのコンポーネント設定を再起動する:

```
# drweb-ctl reload
```

このアクションを実行するにはスーパーユーザー権限が必要です。権限を昇格させるには、以下の例のようにsudoコマンドを使用できます。

```
$ sudo drweb-ctl reload
```

6. サーバー証明書が/home/user/cscert.pemファイルである場合に、ホスト192.168.0.1で動作している集中管理サーバーにDr.Web for UNIX Internet Gatewaysを接続する:

```
$ drweb-ctl esconnect 192.168.0.1 --Certificate /home/user/cscert.pem
```

7. settings.cfg設定ファイルを使用して、Dr.Web for UNIX Internet Gatewaysを集中管理サーバーに接続する:

```
$ drweb-ctl esconnect --cfg <path to the settings.cfg file>
```

8. Dr.Web for UNIX Internet Gatewaysを集中管理サーバーから切断する:

```
# drweb-ctl esdisconnect
```

このアクションを実行するにはスーパーユーザー権限が必要です。権限を昇格させるには、以下の例のようにsudoコマンドを使用できます。

```
$ sudo drweb-ctl esdisconnect
```

9. drweb-updateコンポーネントとdrweb-configdコンポーネントによってDr.Web for UNIX Internet Gatewaysのログに作成された最後のログレコードを表示する:

```
# drweb-ctl log -c Update,ConfigD
```

3. 脅威の管理

1. 検出された脅威に関する情報を表示します。

```
$ drweb-ctl threats
```

2. 駆除されていない脅威を含むファイルをすべて隔離へ移動します。

```
$ drweb-ctl threats --Quarantine All
```

3. 隔離へ移されたファイルのリストを表示します。



```
$ drweb-ctl quarantine
```

4. 隔離からすべてのファイルを復元します。

```
$ drweb-ctl quarantine --Restore All
```

4. 自律コピーモードでの動作例

1. 自律コピーモードでファイルをスキャンし、隔離します。

```
$ drweb-ctl scan /home/user -a --OnKnownVirus=Quarantine  
$ drweb-ctl quarantine -a --Delete All
```

最初のコマンドは自律コピーモードで/home/userディレクトリにあるファイルをスキャンします。既知のウイルスが含まれるファイルは隔離に移されます。2番目のコマンドは隔離コンテンツを(自律コピーモードでも)処理し、すべてのオブジェクトを削除します。

設定パラメータ

コマンドラインから製品を管理するためのDr.Web Ctlツールの場合、Dr.Web for UNIX Internet Gatewaysの統合された[設定ファイル](#)には、パラメータを含む独自のセクションはありません。設定ファイルの[Root] [セクション](#)に指定されているパラメータを使用します。



Dr.Web 管理Webインターフェース

このセクションの内容:

- [機能](#)
- [コンポーネントを管理する](#)
- [脅威の管理](#)
- [設定を管理する](#)
- [ローカルファイルをスキャンする](#)

機能

Dr.Web for UNIX Internet GatewaysのWebインターフェースでは、以下の操作が可能です。

1. Dr.Web for UNIX Internet Gatewaysコンポーネントの現在の状態を表示し、一部のコンポーネントを起動または停止します。
2. 更新のステータスを表示し、必要に応じて手動で更新プロセスを開始します。
3. 製品ライセンスのステータスを表示し、必要に応じてライセンスキーを読み込みます。
4. 検出された脅威のリストを表示し、隔離されたオブジェクトを管理します ([Dr.Web File Checker](#)コンポーネントを使用してローカルファイルシステムで検出された脅威のみが表示されます)。
5. Dr.Web for UNIX Internet Gatewaysに含まれるコンポーネントの設定を編集します。
6. Dr.Web for UNIX Internet Gatewaysを集中管理サーバーに接続したり、スタンドアロンモードに切り替えたりします。
7. ローカルファイルのオンデマンドスキャンを開始します (ブラウザで開いたページにファイルをドラッグ&ドロップして実行する機能も含まれます)。

Webインターフェースのシステム要件

以下のWebブラウザでは、Webインターフェースが正常に動作することが保証されています。

- Microsoft Internet Explorer - バージョン11以降
- Mozilla Firefox - バージョン25以降
- Google Chrome - バージョン30以降

Webインターフェースにアクセスする

Webインターフェースにアクセスするには、ブラウザのアドレスバーに次のアドレスを入力します。

```
https:// <host_with_drweb>: <port>/
```

ここで、<host_with_drweb>は、Dr.Web for UNIX Internet GatewaysがDr.Web HTTPD Webインターフェースサーバーで動作するホストのIPアドレスまたは名前で、<port>は、Dr.Web HTTPDがリスンしている (このホスト上の) ポートです。ローカルホスト上で動作するDr.Web for UNIX Internet Gatewaysコンポーネントにアクセスするには、IPアドレス127.0.0.1または名前localhostを使用します。[デフォルト](#)では、<port>は4443です。



したがって、デフォルトではローカルホストのWebインターフェースにアクセスするために、ブラウザのアドレスバーに次のURLを入力します。

```
https://127.0.0.1:4443/
```

管理サーバーへの接続が確立されると、スタートページが開き、認証フォームが表示されます。管理機能にアクセスするには、Dr.Web for UNIX Internet Gatewaysが動作しているホスト上で管理権限を持つユーザーのログインとパスワードを指定して、認証フォームに入力します。

必要に応じて、個人ユーザー証明書を使用してWebインターフェースで認証を提供できます。それを行うには：

1. 認証局証明書で署名された個人証明書を作成します。
2. 管理用のWebインターフェースに接続するために使用されるブラウザで、署名済み証明書をユーザー認証証明書としてインポートします。
3. Dr.Web HTTPDの[設定](#) (パラメータAdminSslCA)で、個人証明書に署名する認証局証明書へのパスを指定します。

Webインターフェースでの許可に個人ユーザー証明書を使用する場合、許可フォームは表示されず、ユーザーはrootとして許可されます。

必要に応じて、[付録E. SSL証明書を生成する](#)のセクションを参照してください。

メインメニュー

認証に成功すると表示されるWebインターフェースの左ペインにメインメニューがあります。そのメニューアイテムでは以下の操作を実行できます。

- **メイン** - Dr.Web for UNIX Internet Gatewaysのインストール済みコンポーネントとそのステータスの全リストを表示する[メインページ](#)を開きます。
- **脅威** - サーバー上で検出された[すべての脅威を表示する](#)ページを開きます。このセクションでは、これらの検出された脅威を管理できます（感染したオブジェクトの隔離、検出された悪意のあるオブジェクトの再スキャン、修復、削除など）。
- **設定** - サーバーにインストールされているDr.Web for UNIX Internet Gatewaysの[コンポーネント設定](#)のページを開きます。
- **情報** - このWebインターフェースのバージョンとウイルスデータベースの状態に関する簡単な情報を表示するページを開きます。
- **ヘルプ** - Dr.Web for UNIX製品のヘルプ情報を含む新しいブラウザタブを開きます。
- **ファイルをスキャン** - [ファイルをすばやくスキャンする](#)ためのパネルを表示します。このパネルは、閉じられるまでWebインターフェースの開いているページの上部に表示されます。
- **ログアウト** - 現在のWebインターフェースセッションを終了します（ユーザーの個人証明書による認証には使用できません）。

コンポーネントを管理する

メインページでは、Dr.Web for UNIX Internet Gatewaysに含まれるコンポーネントのリストを表示したり、それらの動作を管理したりすることができます。



リスト上にあるDr.Web for UNIX Internet Gatewaysのコンポーネントは、脅威を監視するメインコンポーネントと、Dr.Web for UNIX Internet Gatewaysが正常に動作するよう全体的に管理するサービスコンポーネントの2つのグループに分けられます。メインコンポーネントのリストは、ページ上部に表形式で表示されます（コンポーネントのリストは、ディストリビューション範囲によって異なります）。コンポーネントごとに、以下の情報が表示されます。

1. **名前**。表示されているコンポーネント名をクリックすると、そのコンポーネントの[設定ページ](#)が開きます。
2. **状態**。コンポーネントの状態は、スイッチアイコンとコンポーネントの現在の状態に関するメモによって示されます。スイッチをクリックするだけで、コンポーネントを開始または中断できます。スイッチの状態には次のようなものがあります。

	- コンポーネントが無効になっているため、使用されていません。
	- コンポーネントが有効になっており、正しく動作しています。
	- コンポーネントは有効になっていますが、エラーにより動作していません。

コンポーネントの動作中にエラーが発生した場合は、コンポーネントの状態に関するメモではなく、エラーメッセージが表示されます。 アイコンをクリックすると、発生したエラーに関する詳細情報とエラーを解決するための推奨事項がウィンドウに表示されます。

3. **読み込み**。過去1分間、5分間、15分間に、コンポーネントによって1秒間に処理されたファイルの平均数がそれぞれ表示されます（3つの数字がスラッシュ「/」で区切られて表示されます）。
4. **エラー**。過去1分間、5分間、15分間にコンポーネントで1秒間に検出されたエラーの平均数がそれぞれ表示されます（3つの数字がスラッシュ「/」で区切られて表示されます）。

ツールチップを表示するには、 アイコンの上にカーソルを置きます。

メインコンポーネントに関する情報がまとめられた表の下に、Dr.Web for UNIX Internet Gatewaysのサービスコンポーネント（[スキャンエンジン](#)、[ファイルスキャンコンポーネント](#)など）がタイル表示されます。サービスコンポーネントごとに、その状態と動作統計も表示されます。これらのコンポーネントの設定ページを開くには、目的のコンポーネントの名前をクリックします。通常、これらのコンポーネントは必要に応じて自動的に起動または停止されます。ユーザーによって手動で起動および停止される可能性があるサービスコンポーネントについては、名前と動作統計の他に、コンポーネントを起動および停止するためのスイッチも、該当するサービスコンポーネントのタイルに表示されます。

ページの下部には、ウイルスデータベースが最新かどうかという情報と、[ライセンス](#)情報が表示されます。ウイルスデータベースを強制的に更新するには、[更新](#)をクリックします。[更新ボタン](#)（またはライセンスの現在の状態によっては[ライセンスを有効化ボタン](#)）をクリックすると、Dr.Web for UNIX Internet Gatewaysに対して有効なキーファイルをライセンスサーバーにアップロードしてライセンスを更新または有効化できます。

脅威の管理

脅威ページで、検出された脅威の一覧を表示し、それらに対する対応を管理できます。

このページには、ファイルシステムを監視およびスキャンするDr.Web for UNIX Internet Gatewaysのコンポーネントによって検出された脅威のすべてのリストが含まれています。ページ上部には、カテゴリ別に脅威にフィルターを適用できるメニューがあります。

- **全て** - 検出されたすべての脅威（アクティブな脅威と隔離された脅威の両方を含む）を表示します。
- **アクティブ** - アクティブな（検出されたがまだ駆除されていない）脅威のみを表示します。



- **ブロック済** - ブロックされているすべての脅威、つまり駆除されていないが、それを含む感染オブジェクトがブロックされている脅威をすべて表示します。
- **隔離済** - 隔離に移された脅威を表示します。
- **エラー** - エラーのために処理されなかった脅威を示します。

上部メニューの脅威カテゴリーの名称の隣(右側)には、このカテゴリーに分類される検出済みの脅威の数が表示されます。そのカテゴリーに属する脅威が現在表示され、選択されているカテゴリーは、暗い色のフォントで強調されています。必要なカテゴリーの脅威を表示するには、メニューのカテゴリーの名前をクリックしてください。



ネットワークトラフィックをスキャンするコンポーネント ([SpIDer Gate](#)、[Dr.Web ICAPD](#))、および [Dr.Web ClamD](#)によって検出された脅威は脅威ページに表示されません。これらのコンポーネントによって検出された脅威を追跡するために、SNMPを介して使用可能な脅威カウンターと追跡通知を制御できます ([Dr.Web SNMPD](#)はMIB [Dr.Web構造](#)に従って脅威カウンターと通知へのアクセスを付与します)。

脅威ごとに次の情報が一覧表示されています。

- **ファイル** - 悪意のあるオブジェクトを含むファイルの名前(ファイルパスは指定されていません)。
- **所有者** - 感染ファイルを所有するユーザーの名前。
- **コンポーネント** - 脅威を検出したDr.Web for UNIX Internet Gatewaysのコンポーネントの名前。
- **脅威** - (Doctor Web社の使用する分類に従い) ファイルで検出された脅威の名前。

リストで選択されているオブジェクトについては、以下の情報が表示されます。

- 脅威の名前(Dr.Webウイルス情報ライブラリのページを開くと、その脅威の説明が表示されます)。
- ファイルのサイズ、Byte単位。
- 脅威を検出したコンポーネントの名前。
- 脅威が検出された日時。
- 脅威が最後に変更された日時。
- 感染ファイルを所有しているユーザーの名前。
- ファイルの所有者を含むグループの名前。
- 脅威を含む隔離ファイルに割り当てられた識別子(ファイルが隔離された場合)。
- ファイルの元の場所(脅威の検出時にファイルが存在していた場所)を指すフルパス。



リスト内の任意のオブジェクトをクリックして選択できます。複数のオブジェクトを選択するには、対応するオブジェクトのチェックボックスを選択します。すべてのオブジェクトを選択するか選択をキャンセルするには、脅威リストのヘッダーのファイルフィールドのチェックボックスをオンにします。



リストで選択したオブジェクトにアクションを適用するには、脅威リストの真上にあるツールバーの対応するボタンをクリックします。ツールバーには、次のボタンがあります(選択した脅威の種類によっては、使用できないボタンがあります)。



- 選択したファイルを(永久に)削除します。



	- 選択したファイルを隔離から元の場所に復元します。
	- 選択したファイルに追加のアクションを適用します（使用可能なアクションはドロップダウンリストで指定します）。 <ul style="list-style-type: none">● 隔離 - 脅威を含む選択したファイルを隔離します。● 修復 - 脅威の修復を試みます。● 無視 - 選択したファイルで検出された脅威を無視し、リストからその脅威を削除します。



検索クエリーに基づいて表示された脅威にフィルターを適用することもできます。フィルターを適用して不要な脅威を除外してクエリーに対応するものだけを表示するには、検索ボックスを使用します。検索ボックスはツールバーの右側に  マークと一緒に表示されています。脅威リストにフィルターを適用するには、検索ボックスに単語を入力します。名前や説明に入力した単語が含まれていない脅威はすべて非表示になります（このフィルターの適用では大文字と小文字が区別されません）。検索結果を消去してフィルターを適用していないリストを表示するには、検索ボックスの  をクリックするか、単語を消去します。



設定を管理する

Dr.Web for UNIX Internet Gatewaysに含まれ、[メインページ](#)に一覧表示されているコンポーネントの現在の[設定パラメータ](#)を表示、変更できます。そのためには、[設定ページ](#)を開きます。このページでは、Dr.Web for UNIX Internet Gatewaysを[集中管理](#)モードまたは[スタンドアロン](#)モードに切り替えることもできます（これらのモードの詳細については、[動作モード](#)を参照してください）。

ページの左側に表示されるメニューには、設定を表示、調整できるすべてのDr.Web for UNIX Internet Gatewaysのコンポーネント名が含まれています。任意のコンポーネントの設定を表示、調整するには、まずこのメニューで該当するコンポーネント名をクリックします。現在、設定の表示および編集を行っているコンポーネントの名前は左側のメニューに強調表示されます。

- メニューの集中管理の項目を選択すると、集中管理モードを[管理するページ](#)に移動します。
- メニューの全般設定の項目は、Dr.Web ConfigDコンポーネントの[設定](#)に対応しており、Dr.Web for UNIX Internet Gatewaysの全体的な機能を担っています。

コンポーネントにメイン設定のセクションとは別の追加設定のセクションがある場合（たとえば、ClamAV®アンチウイルスのインターフェースをエミュレートし、異なる接続アドレスを使用するクライアントごとに個別のスキャンパラメータを保持するためにそれらの追加セクションを使用する、Dr.Web ClamDコンポーネントで使用できるセクション）、追加セクションの展開や折りたたみができると示すアイコンがコンポーネント名の左側に表示されます。このアイコンが  の場合、追加セクションは非表示になります。アイコンが  の場合は、追加セクションが1行に1つずつメニューに表示されます。追加セクションのリストを展開したり折りたたんだりするには、目的のコンポーネントの名前の横にある展開・折りたたみアイコンをクリックします。

- 設定を含む追加のセクションは、インデントラインとして表示されます。追加セクションのパラメータを表示または編集するには、その名前をクリックします。
- コンポーネントの設定を含む下位セクションの追加が許可されている場合、コンポーネント名の右側にある  をクリックして追加します。次に、新しいサブセクションに一意の名前（タグ）を指定して、**OK**をクリックします。サブセクションを作成せずにウィンドウを閉じるには、**キャンセル**をクリックします。
- コンポーネントのサブセクションを削除するには、コンポーネント名にカーソルを合わせると表示されるサブセクション名（タグ）の右側の  をクリックします。次に、サブセクションを削除することを確認してはいをクリックするか、**いいえ**をクリックしてサブセクションを削除せずにウィンドウを閉じます。



設定ページの上には、表示モードを変更できるメニューがあります。以下のモードが利用可能です。

- **全て** - 表示および調整可能なすべてのコンポーネントの設定パラメータを含むテーブルを表示します。
- **変更** - デフォルトの値とは異なる値を持つコンポーネントの設定パラメータを含むテーブルを表示します。
- **Ini エディタ** - テキストエディターを表示し、デフォルトの値とは異なる値を持つこのコンポーネントの設定パラメータを示します。表示されるテキストは、**設定ファイル**と同じ形式です (parameter = value のペアを含みます)。

検索クエリーに基づいて表示されたパラメータにフィルターを適用することもできます。フィルターを適用して不要なパラメータを除外し、クエリーに対応するものだけを表示するには、検索ボックスを使用します。検索ボックスは表示モードメニューの右側に 🔍 マークと一緒に表示されています。パラメータリストにフィルターを適用するには、検索ボックスに任意の単語を入力します。説明に入力した単語が含まれていないパラメータはすべて非表示になります (このフィルターの適用では大文字と小文字が区別されません)。検索結果を消去してフィルターを適用していないリストを表示するには、検索ボックスの ✕ をクリックするか、その中の単語を消去します。

パラメータが表形式で表示されている場合 (つまり、全て表示モードと変更表示モード) にのみ、フィルターを適用してパラメータを除外できます。

表形式でコンポーネント設定を表示、編集する

表形式でパラメータを表示する場合 (全て表示モードと変更表示モード)、各表の行にはパラメータの名前と説明 (左側) およびその現在値 (右側) が含まれます。Boolean値パラメータ (使用可能な値が2つのみの場合、「はい」と「いいえ」) では、値の代わりにチェックボックスが表示されます (チェックを入れると「はい」を、チェックしないと「いいえ」を意味します)。



(変更されたものだけでなく) すべてのパラメータを表示するように選択した場合、変更された (デフォルト以外の) 値は太字で示されます。

完全なパラメータリストはグループに分割されます (全般、アドバンスなど)。グループを折りたたむまたは展開するには、その見出し (名前) をクリックします。グループが折りたたまれていて、そのパラメータが表に表示されていない場合は、グループ名の左側に ▶ のアイコンが表示されます。グループが展開されてテーブルにパラメータが表示されると、▼ のアイコンがグループ名の左側に表示されます。

パラメータを調整するには、表内の現在の値をクリックします (Boolean値パラメータの場合は、対応するチェックボックスのチェックマークを設定または削除します)。パラメータに一連の定義済みの値がある場合は、現在の値をクリックした後にすべてドロップダウンリストとして表示されます。パラメータに数値がある場合は、現在の値をクリックした後に編集ボックスが表示されます。必要な値を指定して、ENTERを押してください。以下の図は、パラメータ値を変更する方法の例を示しています (図に示されているコンポーネントのセットは、提供されているものとは異なる可能性があることに注意してください)。パラメータ値に対するすべての変更は、対応するコンポーネントの設定にすぐに適用されます。



Scanning Engine [ScanEngine]

全て 変更 Ini エディタ

▼ 全般

MaxForks 4
スキャンの子プロセスの最大数

LogLevel 通知
コンポーネントのログの詳細レベル

Log Auto
Syslog または 指定されたファイルにログを書き込む

▼ アドバンス

FixedSocketPath 指定されていません
このホスト上の外部クライアントに接続するための UNIXソケット

図3. 表形式のコンポーネント設定

パラメータがその値として文字列を要求しているか、任意の値のリストを受け付ける場合は、パラメータの現在の値をクリックして編集すると、ポップアップウィンドウが表示されます。パラメータが値のリストを受け付ける場合は、次の図に示すように複数行の編集ボックスに表示されます（1行に1つの値）。一覧表示されている値を編集するには、編集ボックスで必要な行を変更、削除、または追加する必要があります。

AdminListen

127.0.0.1:4443

キャンセル 保存

図4. 値リストの編集

パラメータの値を編集したら、**保存**をクリックして変更内容を適用し、ウィンドウを閉じます。変更を適用せずにウィンドウを閉じるには、**キャンセル**をクリックするか、ポップアップウィンドウの右上隅にある **X** のアイコンをクリックします。

テキストエディターでコンポーネントの設定を表示、編集する

Ini エディタモードでパラメータを表示すると、それらは製品の**設定ファイル**と同じ形式（parameter = valueのペア）で表示されます。ここでのパラメータは、設定ファイル（対応するコンポーネントの設定セクション）に直接書き込まれるパラメータの名前です。このモードでは、デフォルト値とは異なる値のパ



ラメータのみが表示されます(つまり、全て表示モードで値が太字で強調されているパラメータ)。以下の図は、このシンプルビューのテキストエディターでパラメータがどのように表示されるかを示しています。

Scanning Engine [ScanEngine]

全て 変更 Ini エディタ

このフィールドには、デフォルトと異なる値が設定されたコンポーネントのパラメータが表示されます。ここでは、設定ファイル内に保存されている形で(<parameter>=<value>ストリングとして)設定パラメータを指定することができます。パラメータをデフォルト値に復元するには、該当する値をエディタから削除してください。各コンポーネントで使用可能な設定パラメータとパラメータのセットに関する詳細はヘルプをご確認ください。

MaxForks=3

行われた変更はまだ保存されていません

保存 リセット

図5. 設定用の組み込みエディター

必要な変更を加えるには、設定ファイルの編集について説明したのと同じ規則に従って、このテキストエディターでテキストを編集します(これにより、左側で強調表示されているコンポーネントの設定を含むセクションのみが変更されます)。必要に応じて、コンポーネントで使用可能な任意のパラメータに新しい値を指定できます。この場合、このパラメータの値はデフォルト設定からエディターに入力した値に変わります。パラメータをデフォルト値にリセットする場合は、このテキストエディターでこのパラメータを含む行を消去してください。変更した場合は、変更を保存するとパラメータはデフォルト値に戻ります。

パラメータ値の編集が終了したら、保存をクリックして変更を適用するか、キャンセルをクリックして変更をキャンセルします。



保存をクリックすると、テキストが検証されます。プログラムは、すべてのパラメータが存在し、それらの設定値が有効であるかどうかを確認します。エラーが発生した場合は、適切なメッセージが表示されます。

パラメータ値を指定するために重要な設定ファイルとその機能の詳細については、[付録D. Dr.Web for UNIX Internet Gateways設定ファイル](#)のセクションを参照してください。

追加情報

- Dr.Web ConfigDの[設定パラメータ](#)(共通設定)
- Dr.Web ICAPDの[設定パラメータ](#)
- SpIDer Gateの[設定パラメータ](#)
- Dr.Web Firewall for Linuxの[設定パラメータ](#)
- Dr.Web ES Agentの[設定パラメータ](#)
- Dr.Web Updaterの[設定パラメータ](#)
- Dr.Web ClamDの[設定パラメータ](#)



- Dr.Web File Checkerの[設定パラメータ](#)
- Dr.Web Scanning Engineの[設定パラメータ](#)
- Dr.Web Network Checkerの[設定パラメータ](#)
- Dr.Web SNMPDの[設定パラメータ](#)
- Dr.Web CloudDの[設定パラメータ](#)
- Dr.Web LookupDの[設定パラメータ](#)
- Dr.Web StatDの[設定パラメータ](#)
- [集中管理モードの管理](#)

集中管理モードの管理

Dr.Web for UNIX Internet Gatewaysは、集中管理サーバーに接続したり、スタンドアロンモードに戻して、製品を集中管理サーバーから切断したりすることができます。集中管理モードを管理できるページを開くには、設定ページの設定メニューから集中管理という項目を選択します。

Dr.Web for UNIX Internet Gatewaysを集中管理サーバーに接続したり、集中管理サーバーとの接続を切断したりするには、このページの該当するチェックボックスを使用します。

集中管理サーバーとの接続

集中管理サーバーへの接続を試みると、画面にポップアップウィンドウが表示されます。このウィンドウでは、集中管理サーバーに接続するためのパラメータを指定する必要があります。

The image shows a dialog box titled "手動で設定" (Manual Settings) with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- A text input field labeled "サーバーのアドレスとポート:" (Server address and port).
- A text input field labeled "サーバー証明書ファイル:" (Server certificate file) with a "参照" (Browse) button to its right.
- A section header "▼ 認証(任意)" (Authentication (optional)).
- A text input field labeled "ワークステーションID:" (Workstation ID).
- A text input field labeled "パスワード:" (Password).
- A checkbox labeled "ワークステーションを「新規端末」として接続" (Connect workstation as "New terminal").
- At the bottom, there are two buttons: "接続" (Connect) and "キャンセル" (Cancel).

図6. 集中管理サーバーとの接続



ウィンドウ上部のドロップダウンリストから、集中管理サーバーとの接続方法を1つ選択します。3つの方法があります。

- *ファイルから読み込む*
- *手動で設定*
- *自動で検出*

*ファイルから読み込む*オプションを選択した場合は、このウィンドウの該当するフィールドで、接続設定を含むファイルへのパスも指定する必要があります。このファイルはアンチウイルスネットワーク管理者によって提供されます。*手動で設定*オプションを選択した場合は、集中管理サーバーのアドレスとポートを指定する必要があります。*手動で設定*または*自動で検出*オプションでは、サーバーのパブリックキー（ネットワーク管理者またはインターネットサービスプロバイダーによって提供されたもの）を含むファイルへのパスを指定することもできます。

また、集中管理サーバーでの認証用のワークステーション識別子 (ID) とパスワードを知っている場合は、認証（任意）セクションでそれらを指定できます。これらのフィールドに入力すると、集中管理サーバーへの接続は、正しいIDとパスワードのペアが入力された場合にのみ成功します。これらのフィールドを空白のままにすると、集中管理サーバーへの接続は、集中管理サーバーによって（サーバーの設定に応じて自動的に、またはアンチウイルスネットワーク管理者によって）承認された場合にのみ確立します。

さらに、ワークステーションを「新規端末」として接続オプションを使用することもできます（新規ユーザーとして接続する場合）。この場合、ワークステーションからの接続に対して集中管理サーバーで新規端末モードが許可されていると、集中管理サーバーはこの接続を承認した後、自動的に一意のIDとパスワードのペアを生成します。その後、コンピューターをサーバーに接続する際はこのペアが使用されます。このモードでは、すでにサーバー上にワークステーションの別のアカウントがある場合でも、集中管理サーバーはワークステーション用に新しいアカウントを生成します。



接続パラメータはアンチウイルスネットワーク管理者またはサービスプロバイダーによって提供された指示に厳密に従って指定してください。

集中管理サーバーに接続するには、すべてのパラメータを指定し、接続をクリックして、接続が確立されるまで待ちます。サーバー接続を確立せずにウィンドウを閉じるには、キャンセルをクリックします。



Dr.Web for UNIX Internet Gatewaysを集中管理サーバーに接続すると、スタンドアロンモードに戻すまで、その動作は集中管理サーバーによって管理されます。Dr.Web for UNIX Internet Gatewaysが起動されるたびに、集中管理サーバーへの接続が自動的に確立されます。

ローカルファイルをスキャンする

Webインターフェースには、ローカルコンピューター（現在Webインターフェースにアクセスしているコンピューター）に保存されているファイルをスキャンして、ファイルに悪意のあるコンテンツが含まれているかどうか確認する機能があります。スキャンにはDr.Web for UNIX Internet Gatewaysに含まれているスキャンエンジンが使用されます。スキャン対象として選択されたファイルはDr.Web for UNIX Internet Gatewaysが動作しているサーバーに（HTTPプロトコル経由で）アップロードされますが、脅威が見つかった場合でも、スキャン後にファイルがサーバーに保存されることも、隔離されることもありません。スキャンするファイルを送信したユーザーには、スキャンの結果についてのみ通知されます。



この機能は、Dr.Web for UNIX Internet GatewaysディストリビューションにDr.Web Network Checkerコンポーネントが含まれている場合のみ使用できます。

ローカルファイルをスキャンするパネルを開いて、スキャン用のパラメータを設定する

Webインターフェースのメインメニューでファイルをスキャン項目を選択したときに表示されるローカルファイルのスキャンパネルを使用して、スキャンするファイルを選択してアップロードできます。起動したパネルは、Webインターフェースの右下隅に表示されます。ローカルファイルのスキャンパネルは以下のようになります。



図7. ローカルファイルのスキャンパネル

このパネルを閉じるには、パネルの右上隅にある **×** をクリックします。**⚙️** アイコンをクリックすると、ローカルファイルのスキャン設定を表示できます。これには、ファイルをスキャンする最大時間(ローカルコンピューターからサーバーにファイルをアップロードするのにかかる時間は含まれません)、ヒューリスティック解析の使用、圧縮されたオブジェクトの最大圧縮率、コンテナ(アーカイブなど)に圧縮されたオブジェクトの最大ネスティングレベルなどが含まれます。



図8. ローカルファイルをスキャンするためのパラメータを設定する

変更した設定を適用して、スキャンするファイルを選択できるファイル選択モードに戻るには、**適用** ボタンを押します。設定に変更を適用せずにファイル選択に戻るには、**キャンセル** ボタンを押します。

ローカルファイルのスキャンを開始する

スキャンするファイルを選択してスキャンを開始するには、ファイルをここにドラッグするか、クリックして選択し、表示されているターゲット領域を左クリックします。そこをクリックすると、各OSのファイルマネージャーの標準的なファイル選択ウィンドウが開きます。スキャン対象として一度に複数のファイルを選択できます。スキャン対象としてディレクトリを選択することはできませんのでご注意ください。ファイルマネージャーウィンドウで選択したファイルをマウスで直接ファイルスキャンパネルのターゲットエリアにドラッグすることもできます。スキャンするファイルを指定すると、Dr.Web for UNIX Internet Gatewaysがインストールされているサーバーへのアップロードが開始されます。ファイルがアップロードされると、スキャンが開始されます。ファイルのアップロードおよびスキャン中に、ファイルスキャンパネルにスキャン手順の全体的な進捗状況が表示されます。



図9. ローカルファイルのスキャンの進捗状況

必要に応じて、停止ボタンを押してスキャンを中止できます。スキャンが完了すると、アップロードされたファイルのスキャンに関するレポートがファイルスキャンパネルに表示されます。



図10. スキャンしたローカルファイルの結果

複数のファイルがアップロードされると、スキャンに関する詳細なレポートが利用可能になります。拡張レポートを表示するには、すべてのファイルについてレポートを見るというリンクをクリックします。



図 11. スキャンしたローカルファイルに関する詳細レポート

レポートを閉じて、パネルでスキャン対象の新しいファイルを選択できる状態に戻るには、**OK**を押します。



ファイルスキャンパネルを閉じているときでも、(スキャンの現在の設定を使用して)ローカルファイルのスキャンを開始することができます。ローカルファイルのアップロードとスキャンを開始するには、ファイルマネージャーウィンドウからブラウザで開いているWebインターフェースのページにドラッグアンドドロップします。



Dr.Web ICAPD

Dr.Web ICAPDコンポーネントはICAPプロトコルを介してHTTPプロキシサーバー（Squidなど）に接続します。通常、HTTPプロキシサーバーは、LANユーザーにインターネットアクセスを提供するために使用されるサーバー（ゲートウェイ）にインストールされます。プロキシサーバーはDr.Web ICAPDを外部フィルターとして使用します。したがって、Dr.Web ICAPDはユーザーのリクエストと、それらのリクエストに対するサーバーのレスポンスを解析します。外部ネットワーク上にあるリソースへのユーザーアクセスを禁止する必要がある場合、または送信データ（ユーザーリクエストまたはサーバーレスポンス）に脅威が含まれているかエラーのためにスキャンできない場合、Dr.Web ICAPDは、Dr.Web ICAPDによってテンプレートから生成される特別なHTMLページをユーザーに返すようにプロキシサーバーに指示します。



HTTPプロトコルを介して転送されるファイルのスキャンの負荷が高まると、Dr.Web Network Checkerコンポーネントが利用できるファイル記述子の数が減少するため、スキャンに問題が生じる場合があります。この場合、Dr.Web for UNIX Internet Gatewaysに利用できるファイル記述子の制限数を増やす必要があります。

動作原理

Dr.Web ICAPDコンポーネントはICAPプロトコル（RFC 3507で説明されている *Internet Content Adaptation Protocol*（インターネットコンテンツアダプテーションプロトコル））を使用して、Dr.Web for UNIX Internet Gatewaysの外部にあり、LANホストからWebサーバーへのHTTP/HTTPS接続を処理するプロキシサーバーと対話します。

ICAPは軽量のHTTPライクなプロトコルです。クライアントはICAPサーバーに対して、ヘッダーと、チェックするためのカプセル化されたHTTPリクエストを含むリクエストを送信します。ICAPサーバーはレスポンスとして、修正されたHTTPリクエストと1つまたは複数のヘッダーを返します。

ICAPのインタラクションでは、次のタイプのリクエスト（メソッド）を使用できます。

- REQMOD - リクエストの検証／修正に使用します。
- RESPMOD - レスポンスの検証／修正に使用します。
- OPTIONS - ICAPサーバーとの接続に関する情報の取得に使用します。

REQMODとRESPMODのリクエストでは、次のヘッダーを使用できます。

- X-Client-IP - HTTPリクエストを送信したクライアントの発信元IPアドレス。
- X-Server-IP - クライアントによって送信されたHTTPリクエストの宛先IPアドレス。
- X-Client-Username - プロキシサーバーで認証されたクライアントの名前（userまたはuser@domainとして指定）。

REQMODリクエストとRESPMODリクエストに対するレスポンスには、次のヘッダーを含めることができます。

- X-Response-Info - リクエストされたWebリソースが危険または望ましくないカテゴリーに属する場合に、レスポンスに含まれます。
- X-Infection-Found - ウイルスやその他の危険なオブジェクトまたは疑わしいオブジェクトに関する情報。
- X-Virus-ID - 検出されたウイルスの名前。
- X-Violations-Found - チェック中に発生したエラーの情報。



OPTIONSリクエストにはDrWeb-Get-Scan-Statusヘッダーが含まれることがあります。このヘッダーの値がYesの場合、Dr.Web Scanning Engine、Dr.Web Core Engine、およびウイルススペースのバージョンに関する情報が返されます。

OPTIONSリクエストに対するレスポンスには、次のヘッダーを含めることができます。

- X-Allow-Out - Dr.Web ICAPDがレスポンスに含めることができるヘッダーフィールドのリスト。
- X-Include - 前回受信したリクエストから取得したヘッダーの値。
- DrWeb-Core-Engine - Dr.Web Core Engineのバージョン。
- DrWeb-Scan-Engine - Dr.Web Scan Engineのバージョン。
- DrWeb-Scan-Status - 現在のスキャン動作のステータス。
- DrWeb-Database-Timestamp - ウイルススペースのタイムスタンプ。
- DrWeb-Virus-Records - ベース内のレコード数。

Dr.Web ICAPDはWebコンテンツをフィルタリングし、潜在的に危険または望ましくないWebリソースへのアクセスをブロックすることがあります。ユーザーが望ましくないリソースをリクエストした場合、テンプレートに従って生成されたブロックページが返されます。このページには、ブロックの理由に関する情報が含まれています。またこのブロックページは、Dr.Web ICAPDがエラーを検出したときや、データのチェック中にエラーが発生したときにも返されません。

このコンポーネントは、URLがいずれかのカテゴリーに属しているかどうかを確認するために、Doctor Webの更新サーバーから定期的に更新されるWebリソースカテゴリーのデータベースを使用するだけでなく、Dr.Web Cloudサービスの参照も行います。Doctor Webは、以下のWebリソースカテゴリーを追跡します。

- *InfectionSource* - 悪意のあるソフトウェアを含むWebサイト(「感染源」)。
- *NotRecommended* - アクセスすることが推奨されない不正なWebサイト(「ソーシャルエンジニアリング」を使用しているもの)。
- *AdultContent* - ポルノまたはエロティックなコンテンツ、出会い系サイトなどを含むWebサイト。
- *Violence* - 暴力行為を助長するWebサイトや、さまざまな死亡事故などに関するコンテンツを含むWebサイト。
- *Weapons* - 武器および爆発物に関するWebサイトや、それらの製造に関する情報を提供しているWebサイト。
- *Gambling* - 勝負事、カジノ、オークションなどのオンラインゲームへのアクセスを提供するWebサイト(賭けサイトなどを含む)。
- *Drugs* - 麻薬の使用、製造または流通などを促進するWebサイト。
- *ObsceneLanguage* - (タイトルや記事などに)卑猥な表現を含むWebサイト。
- *Chats* - テキストメッセージのリアルタイム送信を提供するWebサイト。
- *Terrorism* - 攻撃的なプロパガンダ、またはテロ攻撃などに関する内容を含むWebサイト。
- *FreeEmail* - メール無料登録を提供するWebサイト。
- *SocialNetworks* - さまざまなソーシャルネットワークサービス: 一般、仕事、企業、興味、テーマ別出会い系サイト。
- *DueToCopyrightNotice* - 一部の著作物(映画、音楽など)の著作権者によって定義されるWebサイト。
- *OnlineGames* - インターネットへの常時接続を使用してゲームへのアクセスを提供するWebサイト。



- *Anonymizers* - ユーザーが個人情報を隠し、ブロックされたWebリソースにアクセスすることを可能にするWebサイト。
- *CryptocurrencyMiningPool* - 仮想通貨マイニングのための一般的なサービスへのアクセスを提供するWebサイト。
- *Jobs* - 求人検索Webサイト。

システム管理者は設定で、ユーザーがアクセスすることが望ましくないWebリソースのカテゴリーを指定できます。必要なWebリソースへのアクセスをブロックするために独自のブラックリストを設定したり、ユーザーにアクセスを許可するためにホワイトリストを設定したりすることもできます。ホワイトリストに含まれているWebリソースへのアクセスは、それらが望ましくないカテゴリーに属する場合でも許可されます。ローカルブラックリストとWebリソースカテゴリーのローカルデータベースにURLに関する情報がない場合、プログラムはDr.Web Cloudサービスを参照します。これによりプログラムは、URLの悪質性に関する情報が利用できるかどうか確認できます。このような情報は、Dr.Webの他の製品からリアルタイムで受信されます。



同一のWebサイトを、複数のカテゴリーに同時に所属させることができます。このようなWebサイトへのユーザーアクセスは、そのWebサイトが属する少なくとも1つのカテゴリーが管理者によって望ましくないと設定されている場合はブロックされます。

Webサイトが管理者によってホワイトリストに含まれる場合でも、データ(Webサイトから送信およびダウンロードされたもの)に脅威が含まれているかどうかがスキャンされます。

ICAPプロトコルの特殊な側面のため、データ(.isoイメージ、大きなアーカイブ、ビデオファイルなど)の大部分をスキャンする場合は、長い時間がかかることがあります。スキャンするデータのMIMEタイプに応じて[制限を設定する](#)ことを推奨します。HTTPプロキシサーバーの設定では、ICAPプロトコルによるスキャンのために送信できるデータの最大サイズを制限することも推奨します(プロキシサーバーSquidの[例](#)を参照)。

[Dr.Web Updater](#)コンポーネントは、Doctor Web更新サーバーからWebリソースカテゴリーのデータベースを定期的かつ自動的に更新するために使用されます。同じコンポーネントは、[Dr.Web Scanning Engine](#)スキャンエンジン用のウイルスデータベースの更新にも使用されます。[Dr.Web CloudD](#)コンポーネントはDr.Web Cloudサービスの参照に使用されます(クラウドサービスの使用は付録[共通設定](#)で設定され、必要に応じて無効にできます)。転送されたデータをスキャンするために、Dr.Web ICAPDは[Dr.Web Network Checker](#)コンポーネントを使用します。後者では、[Dr.Web Scanning Engine](#)スキャンエンジンを介してスキャンが開始されます。

HTTPリクエストやレスポンスをブロックまたは通過させるため、Dr.Web ICAPDコンポーネントでは組み込みのルールとLuaスクリプトを使用できます。



Dr.Web ICAPDとHTTPプロキシサーバーの統合については、[Squidプロキシサーバーとの統合のセクション](#)を参照してください。



コマンドライン引数

OSのコマンドラインからDr.Web ICAPDを起動するには、次のコマンドを使用します。

```
$ <opt_dir>/bin/drweb-icapd [<parameters>]
```

Dr.Web ICAPDは次のパラメータを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了します。 短縮形：-h 引数：なし
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了します。 短縮形：-v 引数：なし

例：

```
$ /opt/drweb.com/bin/drweb-icapd --help
```

このコマンドは、Dr.Web ICAPDに関する簡単なヘルプ情報を出力します。

スタートアップノート

このコンポーネントは、自律モードで(他のコンポーネントから自律的に)OSのコマンドラインから直接起動することはできません。必要に応じて[Dr.Web ConfigD](#)設定デーモンによって自動的に起動されます。コンポーネントの動作を管理するには、Dr.Web for UNIX Internet Gateways用のコマンドラインベース管理ツール[Dr.Web Ctl](#)を使用できます(これはdrweb-ctlコマンドを使用して呼び出されます)。



コマンドラインから製品のこのコンポーネントに関するドキュメントを取得するには、`man 1 drweb-icapd`コマンドを使用します。

設定パラメータ

このセクションの内容

- [コンポーネントパラメータ](#)
- [トラフィックモニタリングとアクセスブロックのルール](#)

このコンポーネントは、Dr.Web for UNIX Internet Gatewaysの統合された[設定ファイル](#)の[ICAPD]セクションで指定されている設定パラメータを使用します。



コンポーネントパラメータ

セクションには以下のパラメータが含まれています。

パラメータ	説明
LogLevel <i>{logging level}</i>	コンポーネントの ロギングレベル 。 パラメータの値が指定されていない場合は、[Root] セクション のDefaultLogLevelパラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行パス。 デフォルト値: <opt_dir>/bin/drweb-icapd <ul style="list-style-type: none">GNU/Linuxの場合: /opt/drweb.com/bin/drweb-icapdFreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-icapd
RunAsUser <i>{UID user name}</i>	このパラメータは、その権限によりコンポーネントを実行するユーザーを決定します。ユーザーのUIDまたはログイン情報を指定できます。ログイン情報が数字で構成され、UIDと区別できない場合は、「name:」というプレフィックスを前に付けます(例: RunAsUser = name:123456)。 ユーザー名が指定されていない場合、コンポーネントは、開始後に発生するエラーによって終了します。 デフォルト値: drweb
Start <i>{Boolean}</i>	Dr.Web ConfigD 設定デーモンによってコンポーネントを起動するかどうかを指定します。 このパラメータにYes値を指定すると、設定デーモンはただちにコンポーネントを開始します。また、No値を指定すると、設定デーモンはただちにコンポーネントを終了します。 デフォルト値: No
DebugDumpIcap <i>{Boolean}</i>	詳細なICAPメッセージをデバッグレベルでログファイルに含めず(つまり、LogLevel = DEBUGを設定した場合)。 デフォルト値: No
ListenAddress <i>{network socket}</i>	Dr.Web ICAPDがHTTPプロキシサーバーからの接続をリッスンするネットワークソケット(IPアドレスとポート)を指定します。 デフォルト値: 127.0.0.1:1344
UsePreview	ICAPプレビューモードを有効/無効にします。



パラメータ	説明
<i>{Boolean}</i>	必要でない限り、このパラメータのデフォルト値は 変更しないでください 。 デフォルト値 : Yes
Use204 <i>{Boolean}</i>	ICAPプレビューモードが有効でない場合に、レスポンスコード204を返します。 必要でない限り、このパラメータのデフォルト値は 変更しないでください 。 デフォルト値 : Yes
AllowEarlyResponse <i>{Boolean}</i>	ICAPの早期レスポンスモードを有効にします。つまり、Dr.Web ICAPDがHTTPプロキシサーバーからリクエスト全体を受信する前にクライアントにレスポンスを送信することを許可します。 必要でない限り、このパラメータのデフォルト値は 変更しないでください 。 デフォルト値 : Yes
TemplatesDir <i>{path to directory}</i>	Webリソースをブロックしたときに送信されるHTML通知のテンプレートを含むディレクトリへのパス。 デフォルト値 : <code><var_dir>/templates/icapd</code> <ul style="list-style-type: none">GNU/Linuxの場合 合 : <code>/var/opt/drweb.com/templates/icapd</code>FreeBSDの場合 合 : <code>/var/drweb.com/templates/icapd</code>
Whitelist <i>{domain list}</i>	ドメインのホワイトリスト。このリストに含まれるドメイン(およびそのサブドメイン)は、望ましくないリソースリストに含まれる場合でも、常にユーザーがアクセスできるようになります。 リストの値は、コンマ(引用符内の各値)で区切る必要があります。パラメータはセクションで複数回指定できます(この場合、そのすべての値が1つのリストにまとめられます)。 例 : ドメイン <code>example.com</code> と <code>example.net</code> のリストに追加します。 1. 設定ファイルに値を追加します。 <ul style="list-style-type: none">1行に2つの値 :<pre>[ICAPD] Whitelist = "example.com", "example.net"</pre>2行(1行に1つの値) :<pre>[ICAPD] Whitelist = example.com Whitelist = example.net</pre>



パラメータ	説明
	<p>2. <code>drweb-ctl cfset</code> コマンドを使用して値を追加します。</p> <pre data-bbox="794 315 1442 483"># drweb-ctl cfset ICAPD.Whitelist -a example.com # drweb-ctl cfset ICAPD.Whitelist -a example.net</pre> <div data-bbox="794 510 1442 1003"><p>このパラメータで示されるドメインリストの実際の使用法は、Dr.Web ICAPDに定義されているWebソースへのアクセス管理ルールでの使用方法によって決まります。</p><p>デフォルトルールのリスト (下記参照) は、ブロックされるWebソースカテゴリーのリストのドメインがこのリストに含まれている場合でも、このリストのドメイン (およびそのサブドメイン) へのアクセスが提供されることを保証します。さらに、このデフォルトのルールセットは、ホワイトリストドメインからダウンロードされたデータに脅威が含まれているかどうかをスキャンされることも保証します。</p></div> <p>デフォルト値: (未設定)</p>
Blacklist <i>{domain list}</i>	<p>ドメインのブラックリスト。このリストに含まれるドメイン (およびそのサブドメイン) は、望ましくないリソースリストに含まれていない場合でも、常にユーザーのアクセスがブロックされます。</p> <p>リストの値はコンマで区切ります (各値は引用符で囲みます)。このパラメータはセクションで複数回指定できます (その場合、すべての値が1つのリストにまとめられます)。</p> <p>例: ドメイン <code>example.com</code> と <code>example.net</code> のリストに追加します。</p> <p>1. 設定ファイルに値を追加します。</p> <ul style="list-style-type: none">1行に2つの値: <pre data-bbox="794 1514 1442 1653">[ICAPD] Blacklist = "example.com", "example.net"</pre> <ul style="list-style-type: none">2行 (1行に1つの値): <pre data-bbox="794 1711 1442 1850">[ICAPD] Blacklist = example.com Blacklist = example.net</pre>



パラメータ	説明
	<p>2. drweb-ctl cfset コマンドを使用して値を追加します。</p> <pre data-bbox="778 293 1442 465"># drweb-ctl cfset ICAPD.Blacklist -a example.com # drweb-ctl cfset ICAPD.Blacklist -a example.net</pre>
Adlist <i>{list of strings}</i>	<p>広告URLを表す正規表現のリスト。ここにリストされているいずれかの正規表現に一致するURLは広告URLと見なされます。</p> <p>リストの値は、コンマ(引用符内の各値)で区切る必要があります。パラメータはセクションで複数回指定できます(この場合、そのすべての値が1つのリストにまとめられます)。</p> <p>例: 式「<code>.*ads.+</code>」および「<code>.*ad/.*\.gif\$</code>」をリストに追加します。</p> <ol style="list-style-type: none">設定ファイルに値を追加します。<ul style="list-style-type: none">1行に2つの値:<pre data-bbox="778 1402 1442 1507">[ICAPD] Adlist = ".*ads.+", ".*ad/.*\.gif\$"</pre>2行(1行に1つの値):<pre data-bbox="778 1565 1442 1704">[ICAPD] Adlist = .*ads.+ Adlist = .*ad/.*\.gif\$</pre>drweb-ctl cfset コマンドを使用して値を追加します。<pre data-bbox="778 1765 1442 1933"># drweb-ctl cfset ICAPD.Adlist -a '.*ads.+' # drweb-ctl cfset ICAPD.Adlist -a '.*ad/.*\.gif\$'</pre>



パラメータ	説明
	<p>正規表現は、POSIX構文 (BRE、ERE) またはPerl構文 (PCRE、PCRE2) のいずれかを使用して指定されます。</p> <div data-bbox="778 353 1449 694" style="border: 1px solid #ccc; padding: 10px;"><p> このパラメータで示される式リストの実際の使用方法は、Dr.Web ICAPDに定義されているWebソースへのアクセス管理ルールでの使用方法によって決まります。</p><p>デフォルトルールリスト (以下参照) は、このリストのURLへのアクセスが、これらのURLのドメインがホワイトリストにない場合にのみ、常に禁止されることを保証します。</p></div> <p>デフォルト値: (未設定)</p>
BlockInfectionSource {Boolean}	<p>悪意のあるソフトウェア (<i>InfectionSource</i> カテゴリーに含まれる) を含むWebサイトへの接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <div data-bbox="737 952 1441 1059" style="border: 1px solid #ccc; padding: 5px;"><pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre></div> <p>デフォルト値: Yes</p>
BlockNotRecommended {Boolean}	<p>非推奨サイト (<i>NotRecommended</i> カテゴリーに含まれる) への接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <div data-bbox="737 1310 1441 1417" style="border: 1px solid #ccc; padding: 5px;"><pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre></div> <p>デフォルト値: Yes</p>
BlockAdultContent {Boolean}	<p>アダルトコンテンツ (<i>AdultContent</i> カテゴリーに含まれる) を含むWebサイトへの接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <div data-bbox="737 1668 1441 1776" style="border: 1px solid #ccc; padding: 5px;"><pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre></div> <p>デフォルト値: No</p>
BlockViolence {Boolean}	<p>暴力的描写 (<i>Violence</i> カテゴリーに含まれる) を含むWebサイトへの接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p>



パラメータ	説明
	<pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p>デフォルト値:No</p>
BlockWeapons {Boolean}	<p>武器に関するWebサイト (<i>Weapons</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加します (以下の詳細を参照)。</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p>デフォルト値:No</p>
BlockGambling {Boolean}	<p>ギャンブルのWebサイト (<i>Gambling</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加します (以下の詳細を参照)。</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p>デフォルト値:No</p>
BlockDrugs {Boolean}	<p>麻薬に関するWebサイト (<i>Drugs</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加します (以下の詳細を参照)。</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p>デフォルト値:No</p>
BlockObsceneLanguage {Boolean}	<p>卑猥な表現 (<i>ObsceneLanguage</i>カテゴリーに含まれる)を含むWebサイトへの接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加します (以下の詳細を参照)。</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p>デフォルト値:No</p>
BlockChats {Boolean}	<p>チャットWebサイト (<i>Chats</i>カテゴリーに含まれる)への接続試行をブロックします。</p>



パラメータ	説明
	<p>ブロックをアクティブにするには、次のルールを設定に追加します (以下の詳細を参照)。</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p>デフォルト値: No</p>
BlockTerrorism {Boolean}	<p>テロリズムに関するWebサイト (<i>Terrorism</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加します (以下の詳細を参照)。</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p>デフォルト値: No</p>
BlockFreeEmail {Boolean}	<p>無料メールサービスのWebサイト (<i>FreeEmail</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加します (以下の詳細を参照)。</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p>デフォルト値: No</p>
BlockSocialNetworks {Boolean}	<p>ソーシャルネットワーキングWebサイト (<i>SocialNetworks</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックを有効にするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p>デフォルト値: No</p>
BlockDueToCopyrightNotice {Boolean}	<p>著作権者のリクエストに従って追加されたWebサイトへの接続試行をブロックします。 (<i>DueToCopyrightNotice</i>カテゴリーに含まれるもの)。</p> <p>ブロックを有効にするには、次のルールを設定に追加します (以下の詳細を参照)。</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p>デフォルト値: Yes</p>



パラメータ	説明
BlockOnlineGames {Boolean}	<p>オンラインゲームWebサイト (<i>OnlineGames</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックを有効にするには、次のルールを設定に追加します (以下の詳細を参照)。</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p>デフォルト値: Yes</p>
BlockAnonymizers {Boolean}	<p>アノマイザー (<i>Anonymizers</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックを有効にするには、次のルールを設定に追加します (以下の詳細を参照)。</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p>デフォルト値: Yes</p>
BlockCryptocurrencyMiningPools {Boolean}	<p>仮想通貨マイニングのための一般的なサービスへのアクセスを提供するWebサイト (<i>CryptocurrencyMiningPool</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックを有効にするには、次のルールを設定に追加します (以下の詳細を参照)。</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p>デフォルト値: Yes</p>
BlockJobs {Boolean}	<p>求人検索Webサイト (<i>Jobs</i>カテゴリーに含まれます)への接続試行をブロックします。</p> <p>ブロックを有効にするには、次のルールを設定に追加します (以下の詳細を参照)。</p> <pre>url_category in "ICAPD.BlockCategory" : BLOCK as _match</pre> <p>デフォルト値: No</p>
ScanTimeout {time interval}	<p>Dr.Web ICAPDによって開始された1つのファイルに対するスキャンのタイムアウト。</p> <p>指定可能な値: 1秒 (1s) から1時間 (1h) まで。</p> <p>デフォルト値: 30s</p>
HeuristicAnalysis {On / Off}	<p>未知の脅威を検出するためのヒューリスティック解析を有効/無効にします。ヒューリスティック解析を使用すると保護レベル</p>



パラメータ	説明
	<p>が上がりますが、スキャン時間が長くなります。</p> <p>ヒューリスティックアナライザによって検出された脅威に適用されるアクションは、BlockSuspiciousパラメータ値として指定します。</p> <p>使用可能な値：</p> <ul style="list-style-type: none">• On - ヒューリスティック解析を有効にします。• Off - ヒューリスティック解析を無効にします。 <p>デフォルト値：On</p>
PackerMaxLevel <i>{integer}</i>	<p>圧縮されたオブジェクトの最大ネスティングレベル。圧縮されたオブジェクトは、特別なソフトウェア(UPX、PELock、PECompact、Petite、ASPack、Morphineなど)で圧縮された実行コードです。そのようなオブジェクトには、圧縮されたオブジェクトなども含まれている、他の圧縮されたオブジェクトが含まれる場合があります。このパラメータの値はネスティングの上限を指定します。この上限を超えると、他の圧縮されたオブジェクト内の圧縮されたオブジェクトはスキャンされません。</p> <p>ネスティングレベルの制限はありません。値を0に設定すると、ネストされたオブジェクトはスキャンされません。</p> <p>デフォルト値：8</p>
ArchiveMaxLevel <i>{integer}</i>	<p>他のアーカイブが含まれる可能性のあるアーカイブ(zip、rarなど)の最大ネスティングレベル(これらのアーカイブには他のアーカイブなどが含まれる場合もあります)。このパラメータの値はネスティングの上限を指定します。この上限を超えると、他のアーカイブに含まれるアーカイブはスキャンされません。</p> <p>ネスティングレベルの制限はありません。値を0に設定すると、ネストされたオブジェクトはスキャンされません。</p> <p>デフォルト値：0</p>
MailMaxLevel <i>{integer}</i>	<p>他のファイルが含まれる可能性のあるメーラーのファイル(pst、tbbなど)の最大ネスティングレベル(これらのファイルには他のファイルなどが含まれる場合もあります)。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他のオブジェクト内のオブジェクトはスキャンされません。</p> <p>ネスティングレベルの制限はありません。値を0に設定すると、ネストされたオブジェクトはスキャンされません。</p> <p>デフォルト値：0</p>
ContainerMaxLevel <i>{integer}</i>	<p>他のオブジェクトが含まれる他のタイプのオブジェクト(HTMLページ、jarファイルなど)の最大ネスティングレベル。このパラメータの値はネスティングの上限を指定します。この上限を超えると、他のオブジェクト内のオブジェクトはスキャンされません。</p> <p>ネスティングレベルの制限はありません。値を0に設定すると、ネストされたオブジェクトはスキャンされません。</p>



パラメータ	説明
	デフォルト値: 8
MaxCompressionRatio {integer}	圧縮されたオブジェクトの最大圧縮率（非圧縮サイズと圧縮サイズの比率）。オブジェクトの比率が制限を超えると、そのオブジェクトはDr.Web ICAPDによって開始されたデータのスキャン中にスキップされます。 圧縮率には2よりも小さい値は指定できません。 デフォルト値: 500
BlockKnownVirus {Boolean}	既知の脅威を含むデータの受信または送信をブロックします。 ブロックを有効にするには、次のルールを設定に追加します（ 以下 の詳細を参照）。 <pre>threat_category in "ICAPD.BlockThreat" : BLOCK as _match</pre> デフォルト値: Yes
BlockSuspicious {Boolean}	未知の脅威（ヒューリスティックアナライザによって検出されたもの）を含むデータの受信または送信をブロックします。 ブロックを有効にするには、次のルールを設定に追加します（ 以下 の詳細を参照）。 <pre>threat_category in "ICAPD.BlockThreat" : BLOCK as _match</pre> デフォルト値: Yes
BlockAdware {Boolean}	アドウェアを含むデータの受信または送信をブロックします。 ブロックを有効にするには、次のルールを設定に追加します（ 以下 の詳細を参照）。 <pre>threat_category in "ICAPD.BlockThreat" : BLOCK as _match</pre> デフォルト値: Yes
BlockDialers {Boolean}	ダイヤラープログラムを含むデータの受信または送信をブロックします。 ブロックを有効にするには、次のルールを設定に追加します（ 以下 の詳細を参照）。 <pre>threat_category in "ICAPD.BlockThreat" : BLOCK as _match</pre> デフォルト値: Yes



パラメータ	説明
BlockJokes <i>{Boolean}</i>	<p>ジョークプログラムを含むデータの受信または送信をブロックします。</p> <p>ブロックを有効にするには、次のルールを設定に追加します (以下の詳細を参照)。</p> <pre>threat_category in "ICAPD.BlockThreat" : BLOCK as _match</pre> <p>デフォルト値: No</p>
BlockRiskware <i>{Boolean}</i>	<p>リスクウェアを含むデータの受信または送信をブロックします。</p> <p>ブロックを有効にするには、次のルールを設定に追加します (以下の詳細を参照)。</p> <pre>threat_category in "ICAPD.BlockThreat" : BLOCK as _match</pre> <p>デフォルト値: No</p>
BlockHacktools <i>{Boolean}</i>	<p>ハッキングツールを含むデータの受信または送信をブロックします。</p> <p>ブロックを有効にするには、次のルールを設定に追加します (以下の詳細を参照)。</p> <pre>threat_category in "ICAPD.BlockThreat" : BLOCK as _match</pre> <p>デフォルト値: No</p>
BlockUnchecked <i>{Boolean}</i>	<p>スキャンできないデータの受信または送信をブロックします。</p> <p>デフォルト値: No</p>
MessageHook <i>{path to file Lua function}</i>	<p>LuaでHTTPメッセージを処理するためのスクリプトまたはそのスクリプトを含むファイルへのパス (LuaでのHTTPメッセージ処理セクションを参照)。</p> <p>Lua関数またはファイルパスが指定されていない場合、メッセージはルールに従って処理されます。指定したファイルが利用できない場合、コンポーネントの起動時にエラーが返されます。</p> <p>デフォルト値: <i>自動的に生成されます</i>。デフォルト設定では、次のようなスクリプトになります。</p> <pre>local dw = require "drweb" local cfg = require "drweb.config" local dwl = require "drweb.lookup" local rx = require "drweb.regex" function message_hook(ctx) if ctx.direction == "request" then local url = ctx.request.url</pre>



パラメータ	説明
	<pre>if url.in_list(cfg.blacklist) then return "block" end if not url.in_list(cfg.whitelist) then if rx.search(cfg.adlist, url) or rx.search(cfg.adlist, url.raw) then return "block" end if url.in_categories(cfg.block_url_categories) then return "block" end end end if ctx.body.has_threat{category = cfg.block_threats} then return "block" end if cfg.block_unchecked and ctx.body.scan_error then return "block" end return "pass" end</pre>

トラフィックモニタリングとアクセスブロックのルール

このセクションには、上記のパラメータの他、7つのルールセットRuleSet*(RuleSet0、...、RuleSet6)も含まれます。これらは、トラフィックスキャン、Webリソースへのユーザーアクセスのブロック、インターネットからのコンテンツのダウンロードのブロックを直接管理します。条件の一部の値(IPアドレス範囲、Webサイトカテゴリーのリスト、Webソースのホワイト/ブラックリストなど)については、テキストファイルから読み込まれる値の置き換えがあり、LDAPを介して外部データソースから抽出されます([Dr.Web LookupD](#)コンポーネントを使用)。接続を設定する際には、最終的な解決を含むルールが見つかるまで、すべてのルールが昇順で検査されます。ルールリストのギャップは無視されます。

ルールについては、付録Dの[トラフィックモニタリングのルール](#)のセクションで詳しく説明されています。

ルールを表示して編集する

ルールリストを簡単に編集するために未設定のものが残されています。つまり、ルールが指定されていないRuleSet <i>が</i>あります(<i>- RuleSet</i>ルールセット番号)。RuleSet <i>以外の項目を追加することはできませんが、RuleSet <i>の要素内のルールは追加および削除できます。ルールの表示と編集は、次のいずれかの方法で実行できます。

- (任意のテキストエディターで) [設定ファイル](#)設定ファイルを表示して編集する(このファイルにはデフォルトとは異なる値のパラメータのみが保存されます)。
- [Web管理インターフェース](#)を使用する(インストールされている場合)。
- コマンドラインベースのインターフェース[Dr.Web Ctl](#)(drweb-ctl cfshowおよびdrweb-ctl cfset [コマンド](#))を使用する。



ルールを編集して設定ファイルを変更した場合は、その変更を適用するためにDr.Web for UNIX Internet Gatewaysを再起動します。それには`drweb-ctl reload`コマンドを使用します。

ルールを表示するには、`drweb-ctl cfshow`コマンドを使用します。

ルールセット`ICAPD.RuleSet1`のコンテンツを表示するには、次のコマンドを使用します。

```
# drweb-ctl cfshow ICAPD.RuleSet1
```

ルールを編集するには、`drweb-ctl cfset`コマンドを使用します(以降、`<rule>`はルールのテキストです)。

- `ICAPD.RuleSet1`セットのすべてのルールを新しいルールに置き換えます。

```
# drweb-ctl cfset ICAPD.RuleSet1 '<rule>'
```

- `ICAPD.RuleSet1`ルールセットに新しいルールを次のように追加します。

```
# drweb-ctl cfset -a ICAPD.RuleSet1 '<rule>'
```

- `ICAPD.RuleSet1`セットから特定のルールを次のように削除します。

```
# drweb-ctl cfset -e ICAPD.RuleSet1 '<rule>'
```

- `ICAPD.RuleSet1`ルールセットを次のようにデフォルトの状態にリセットします。

```
# drweb-ctl cfset -r ICAPD.RuleSet1
```

`drweb-ctl`ツールを使用してルールのリストを編集するときは、追加するルールのテキストを一重引用符または二重引用符で囲み、ルール自体のテキストに二重引用符が含まれている場合には、ルールのテキスト内にある二重引用符の前にバックスラッシュ(「\」)をエスケープ文字として使用します。

設定の`RuleSet`変数には、ルールの格納について次のような特徴があります。

- 無条件ルールを追加するときは、条件部分とコロンを省略できます。ただし、そのようなルールは常にルールのリストに文字列「 : `<action>`」として格納されます。
- 複数のアクションを含むルール(「`<condition>` : `<action 1>`, `<action 2>`」など)を追加すると、そのようなルールは基本ルールのチェーン「`<condition>` : `<action 1>`」と「`<condition>` : `<action 2>`」に変更されます。
- ロギングまたはルールは、条件部分で条件の離接(論理和)を許可しないため、論理和を実装するには、各ルールに離接語条件がある条件で一連のルールを記録する必要があります。

接続をスキップするための無条件ルール(Passアクション)を`ICAPD.RuleSet1`セットに追加するには、次のコマンドのみを実行します。

```
# drweb-ctl cfset -a ICAPD.RuleSet1 'Pass'
```




ただし、指定したルールセットからこのルールを削除するには、次のコマンドを実行する必要があります。

```
# drweb-ctl cfset -e ICAPD.RuleSet1 ' : Pass'
```

ICAPD.RuleSet1ルールを、接続用の標準テンプレートへのパスを未解決アドレスから変更してブロックを実行するルールセットに追加するには、次のコマンドを実行する必要があります。

```
# drweb-ctl cfset -a ICAPD.RuleSet1 'src_ip not in file("/etc/trusted_ip") :  
set http_template_dir = "mytemplates", Block'
```

ただし、このコマンドでは指定したセットに2つのルールが追加されるため、ルールのセットからこれらのルールを削除するには、次の2つのコマンドを実行する必要があります。

```
# drweb-ctl cfset -e ICAPD.RuleSet1 'src_ip not in file("/etc/trusted_ip") :  
set http_template_dir = "mytemplates"  
# drweb-ctl cfset -e ICAPD.RuleSet1 'src_ip not in file("/etc/trusted_ip") :  
Block'
```

「悪意のあるオブジェクト *KnownVirus* や *Terrorism* カテゴリに該当するURLが検出された場合はブロックする」などのルールをICAPD.RuleSet1ルールセットに追加するには、このルールセットに次の2つのルールを追加する必要があります。

```
# drweb-ctl cfset -a ICAPD.RuleSet1 'threat_category in (KnownVirus) : Block  
as _match'  
# drweb-ctl cfset -a ICAPD.RuleSet1 'url_category in (Terrorism) : Block as  
_match'
```

ルールのセットからこれらのルールを削除する場合にも、2つのコマンドを実行する必要があります(上記の例を参照)。

デフォルトのルールセット

デフォルトでは、次のブロックルールセットが指定されています。

```
RuleSet0 =  
RuleSet1 = direction request, url_host in "ICAPD.Blacklist" : BLOCK as  
BlackList  
RuleSet1 = direction request, url_host not in "ICAPD.Whitelist", url match  
"ICAPD.Adlist" : BLOCK as BlackList  
RuleSet2 =  
RuleSet3 = direction request, url_host not in "ICAPD.Whitelist",  
url_category in "ICAPD.BlockCategory" : BLOCK as _match  
RuleSet4 =  
RuleSet5 = threat_category in "ICAPD.BlockThreat" : BLOCK as _match  
RuleSet6 =
```

最初の2つのルールは送信HTTP接続を処理します。接続が試みられるホスト(またはURL)がブラックリストに含まれている場合、その接続はブラックリストに基づいてブロックされ、それ以上のスキャンは実行されません。ホスト(URL)がホワイトリストに含まれておらず、アクセスするのが望ましくないマークされているWebサイトカテゴリに属しているか、広告URLを表す正規表現のいずれかに一致する場合、URLは望ましくないカテゴリに属しているため、接続はブロックされます。



RuleSet5で指定されたルールは、(設定に従って)ブロックする必要がある脅威カテゴリに属する脅威のHTTPリクエストまたはレスポンスをスキャンします。そのような脅威がある場合、接続は脅威の検出に基づいてブロックされます。方向条件が指定されていないため、デフォルトでは、クライアントリクエスト(*request*)とサーバーレスポンス(*response*)の両方が検査されます。

トラフィックモニタリングとアクセスブロックのルールの例

1. IPアドレス範囲が10.10.0.0~10.10.0.254のユーザーにChats以外のすべてのカテゴリのWebサイトへのアクセスを許可する。

```
src_ip in (10.10.0.0/24), url_category not in (Chats) : PASS
```

ルール

```
url_host in "ICAPD.Blacklist" : BLOCK as BlackList
```

が、指定されたルールより上記のルールリストに割り当てられている場合、IPアドレス範囲が10.10.0.0~10.10.0.254のユーザーは、ブラックリストのドメイン、つまりパラメータICAPD.Blacklistにリストされているドメインへのアクセスもブロックされます。また、このルールが下記に割り当てられている場合、IPアドレス範囲が10.10.0.0~10.10.0.254のユーザーは、ブラックリストのWebサイトにもアクセスできます。

PASSの処理は最終的なものであるため、これ以上のルールはチェックされず、したがってダウンロードされたデータのウイルススキャンも実行されません。IPアドレス範囲が10.10.0.0~10.10.0.254のユーザーに、ブラックリストに含まれていないChats以外のすべてのカテゴリのWebサイトへのアクセスを許可し、同時に脅威のダウンロードをブロックするには、次のルールを使用します。

```
url_category not in (Chats), url_host not in "ICAPD.Blacklist",  
threat_category not in "ICAPD.BlockCategory" : PASS
```

2. ビデオファイルのコンテンツ(つまり、MIMEタイプが「video/*」のデータ(*はMIMEクラスvideoの任意のタイプ))のスキャンを実行しない。

```
content_type in ("video/*") : PASS
```

LuaでのHTTPメッセージ処理

このセクションの内容

- [概要](#)
- [メッセージ処理のためのスクリプト](#)
- [スクリプトで使用されるテーブル](#)
- [利用可能な補助モジュール](#)

概要

Dr.Web ICAPDコンポーネントはLuaプログラムインタプリタを介したインタラクションをサポートします(バージョン5.3.4を使用。Dr.Web for UNIX Internet Gatewaysに同梱)。Luaで記述されたスクリプトは、HTTPプロトコルメッセージの解析と処理のためにコンポーネントで使用できます。



ICAPプロトコルを介してプロキシサーバーからスキャンのために受信したHTTPメッセージ(リクエストまたはレスポンス)の解析は、Dr.Web ICAPDの設定でMessageHookパラメータの値として指定されたLuaスクリプト(Luaコードのスニペットか、必要な処理プログラムを含むファイルへのパスで指定できる)を使用して実行されます。

メッセージ処理のためのスクリプト

スクリプトの必要条件

このスクリプトには、メッセージスキャンモジュールのエントリーポイントとなるグローバル関数が含まれている必要があります(Dr.Web ICAPDは、新たに受信したメッセージを処理する際にこの関数を呼び出します)。処理関数は、次の呼び出し規則を満たす必要があります。

1. 関数名はmessage_hookです。
2. 引数はMessageContextテーブルのみです(関数から処理されたメールメッセージに関する情報へのアクセス権限を提供します)。
3. 戻り値は文字列です。戻り値は、スキャンされたメッセージの判定、つまり、メッセージをスキップするかブロックするかを決定します。以下の値を使用できます。
 - "pass"では、メッセージが受信者に渡されます(サーバーへのHTTPリクエスト、クライアントへのHTTPレスポンス)。
 - "block"は、HTTPメッセージは受信者に送信されず、クライアントはブロックされたWebページを含むHTTPレスポンスを受信します。

関数の実行時に異なる値が返された場合やエラーが発生した場合は、スキャンエラーとして扱われます。この場合のクライアントへのレスポンスは、BlockUnchecked設定パラメータの値によって異なります。

スキャンのために受信したすべてのHTTPメッセージについて、Dr.Web ICAPDにPass判定を常に返す正しい関数定義の例は以下のとおりです(以降、ctx引数はMessageContextテーブルのインスタンスです)。

```
function message_hook(ctx)
    return "pass"
end
```

次に示す例のスクリプトは、Active DirectoryのWeb Adminsグループのメンバー以外のすべてのユーザーに対して、Dr.WebドキュメントWebサイト以外のすべてのリソースへのアクセスをブロックします。



```
local dwl = require "drweb.lookup"

function message_hook(ctx)

    -- Not to block access to resources at the document website
    -- of Doctor Web
    if ctx.req.url.in_list{"download.geo.drweb.com"} then
        return "pass"
    end

    -- To allow access to users from the WebAdmins group
    -- in Active Directory
    if dwl.check("WebAdmins", "AD@WinRoot", ctx.icap.user) then
        return "pass"
    end

    -- Block access for all the others (to all resources)
    return "block"

end
```

スクリプトで使用されるテーブル

テーブルMessageContext

このテーブルはmessage_hook関数の入力引数として使用され、処理されたHTTPメッセージに関する情報(タイプ、ヘッダー、本文、送信者と受信者に関する情報(ある場合))へのアクセスを提供します。

フィールド	説明	データタイプ
direction	HTTPメッセージタイプ。次の値を取ります。 <ul style="list-style-type: none">"request" - HTTPリクエスト"response" - HTTPレスポンス	文字列
icap	ICAPリクエストヘッダーに関する情報。	テーブル ICAP
request	HTTPリクエストヘッダーに関する情報。	テーブル Request
response	HTTPレスポンスヘッダーに関する情報。	テーブル Response
body	HTTPメッセージ本文に関する情報。	テーブル Body
無効になったメタメソッド: なし		

テーブルICAP

このテーブルはMessageContextテーブルのicapフィールドとして使用されます。HTTPプロキシサーバーからのICAPリクエストに関するデータが含まれます。



フィールド	説明	データタイプ
user	ICAPリクエストのX-Client-Usernameヘッダーから取得したユーザーに関する情報。	テーブル User
src	リクエストを送信したクライアントのIPアドレス(プロキシサーバーによって送信されたICAPリクエストのX-Client-IPヘッダーから取得)またはnil(アドレスが不明な場合)。	テーブル IpAddress
field	ICAPリクエストヘッダーの配列。	HeaderField テーブルの配列
search	正規表現を使用してヘッダーを検索する関数。patterns引数(つまり、検索パターン、Perl構文(PCRE)の1つ(文字列)または複数(文字列の配列)の正規表現)を要求し、使用可能なすべてのヘッダーを検索します。引用符で囲まれた文字列を使用する場合は、スラッシュ文字をエスケープする必要があります。 次のブール値を返します。 <ul style="list-style-type: none"> • true - field.name .. ":" .. field.value.decoded文字列が、少なくとも1つのヘッダーに対して指定した少なくとも1つの正規表現と一致する場合。 • false - 一致するものがない場合。 	機能
value	唯一の引数であるヘッダー名(文字列)を要求する関数。指定された名前を持つ最初のヘッダーの値を返します。この名前前のヘッダーがない場合はnilを返します。	機能
無効になったメタメソッド: なし		

テーブルUser

このテーブルにはユーザーの名前とドメインが含まれます。どちらのフィールドもオプションです。

フィールド	説明	データタイプ
user	ユーザー名	文字列
domain	ユーザードメイン	文字列
無効になったメタメソッド: <ul style="list-style-type: none"> • __toString - この関数は、Userコンテンツを文字列(UTF-8)として返します。 • __concat - この関数は、User文字列値と別の文字列を連結します。 		

テーブルHeaderField

このテーブルではHTTPまたはICAPメッセージヘッダーを指定します。

フィールド	説明	データタイプ
name	ヘッダー名。	文字列



フィールド	説明	データタイプ
value	ヘッダー値。	文字列
無効になったメタメソッド: なし		

テーブルRequest

このテーブルではHTTPリクエストのヘッダーを指定します。

フィールド	説明	データタイプ
method	リクエストで使用されたHTTPプロトコルメソッド("POST"など)。ICAPリクエストにHTTPリクエストヘッダーが含まれていない場合はnil。	文字列
url	HTTPリクエストが送信されるリソースのURL。	テーブルUrl
content_type	HTTPリクエストのContent-Typeヘッダーの情報。	ContentTypeテーブル
field	HTTPリクエストヘッダーの配列。	HeaderFieldテーブルの配列
search	正規表現を使用してヘッダーを検索する関数。patterns引数(つまり、検索パターン、Perl構文(PCRE)の1つ(文字列)または複数(文字列の配列)の正規表現)を要求し、使用可能なすべてのヘッダーを検索します。引用符で囲まれた文字列を使用する場合は、スラッシュ文字をエスケープする必要があります。 次のブール値を返します。 <ul style="list-style-type: none">• true - field.name .. ":" .. field.value.decoded文字列が、少なくとも1つのヘッダーに対して指定した少なくとも1つの正規表現と一致する場合。• false - 一致するものがない場合。	機能
value	唯一の引数であるヘッダー名(文字列)を要求する関数。指定された名前を持つ最初のヘッダーの値を返します。この名前のヘッダーがない場合はnilを返します。	機能
無効になったメタメソッド: なし		

テーブルContentType

このテーブルでは、Content-Typeヘッダーから取得する値を指定します。

フィールド	説明	データタイプ
type	メッセージ部分のMIMEタイプ	文字列
subtype	メッセージ部分のサブタイプ	文字列
param	次のフィールドを持つテーブル配列形式のヘッダーパラメータ:	テーブル配列



フィールド	説明	データタイプ
	<ul style="list-style-type: none">• nameはパラメータの名前(文字列)です。• valueはパラメータの値(文字列)です。	
match	<p>唯一の引数media_types、つまりMIMEタイプを指定する文字列の配列を要求する関数。リスト内の各文字列は"type/subtype"、"type/*"、"*/*"のいずれかの形式でなければなりません。</p> <p>次のブール値を返します。</p> <ul style="list-style-type: none">• true - 本文のMIMEタイプが指定された文字列(大文字と小文字が区別されない)のいずれかに一致するか、配列に文字列"*/*"が含まれている場合。• false - それ以外の場合。	機能
無効になったメタメソッド:		
<ul style="list-style-type: none">• __tostringは、デコードされたヘッダー値を返す関数です。• __concatは、ヘッダーの復号化された値と文字列を連結する関数です。		

テーブルURL

このテーブルではURLを指定します。

フィールド	説明	データタイプ
scheme	スキーム(プロトコル)プレフィックス(例:"http")。プレフィックスがない場合、値はnilになります。	文字列
host	ホスト名またはIPアドレス(例:"example.com")。ホスト名がない場合、値はnilになります。	文字列
port	ポート番号(例:80)。番号がない場合、値はnilになります。	番号
path	リソースへのパス(例:"index.html")。パスがない場合、値はnilになります。	文字列
query	デコードされたリクエストパラメータ。パラメータがない場合、値はnilになります。	文字列
legal_url	URLがowners_noticeカテゴリーに属する場合、フィールドには所有者のWebサイトへのURLが含まれます。属さない場合は、nilになります。	文字列
in_list	<p>唯一の引数hosts、つまりホストリスト(文字列の配列)を要求する関数。次のブール値を返します。</p> <ul style="list-style-type: none">• true - hostが指定されたドメインのいずれかのサブドメインであるか、それらのいずれかに一致する場合。• false - hostが指定されたドメインのいずれかのサブドメインでないか、それらのいずれにも一致しない場合。	機能



フィールド	説明	データタイプ
categories	1つのオプション引数 <code>filter</code> 、つまり <code>UrlCategoryFilter</code> テーブルを受け取る関数 (引数がない場合は、空のテーブルを使用するのと同じです)。フィルターで指定された URL 条件を満たすすべてのカテゴリを反復処理できる、反復子関数を返します。	機能
in_categories	唯一の引数 <code>categories</code> 、つまり URL カテゴリリスト (文字列の配列) を要求する関数。次のブール値を返します。 <ul style="list-style-type: none">• <code>true</code> - URL が指定されたカテゴリの少なくとも1つに該当する場合。• <code>false</code> - URL が、指定されたカテゴリの少なくとも1つに該当しない場合。 <code>categories</code> 配列が空の場合は、常に <code>false</code> を返します。 <code>UrlCategoryFilter</code> テーブルの <code>category</code> フィールドの説明にある可能なカテゴリ値を参照してください。	機能
raw	生のデコードされていない URL。	テーブル <code>RawUrl</code>
無効になったメタメソッド:		
<ul style="list-style-type: none">• <code>__toString</code> - この関数は、<code>Url</code> コンテンツを文字列 (UTF-8) として返します。• <code>__concat</code> - この関数は、<code>Url</code> 文字列値と別の文字列を連結します。		

テーブル `RawUrl`

このテーブルには、デコードされていない URL データが含まれます。

フィールド	説明	データタイプ
scheme	スキーム (プロトコル) プレフィックス (例: "http")。プレフィックスがない場合、値は <code>nil</code> になります。	文字列
host	ホスト名または IP アドレス (例: "example.com")。ホスト名または IP アドレスがない場合、値は <code>nil</code> になります。	文字列
port	ポート番号 (例: 80)。ポート番号がない場合、値は <code>nil</code> になります。	番号
path	リソースへのパス (例: "index.html")。パスがない場合、値は <code>nil</code> になります。	文字列
query	デコードされたリクエストパラメータ。パラメータがない場合、値は <code>nil</code> になります。	文字列
無効になったメタメソッド:		
<ul style="list-style-type: none">• <code>__toString</code> - この関数は、<code>RawUrl</code> コンテンツを文字列 (UTF-8) として返します。• <code>__concat</code> - この関数は、<code>RawUrl</code> 文字列値と別の文字列を連結します。		

テーブル `UrlCategoryFilter`



このテーブルではURLカテゴリーのフィルターを指定します（フィールドはすべてオプションです）。

フィールド	説明	データタイプ
category	URLが該当するカテゴリーのリスト（大文字と小文字は区別されません）。リストには次の値が含まれる場合があります。 <ul style="list-style-type: none">• "infection_source" - 感染源。• "not_recommended" - 非推奨のWebサイト。• "adult_content" - アダルトコンテンツ。• "violence" - 暴力。• "weapons" - 武器。• "gambling" - ギャンブル。• "drugs" - 薬物。• "obscene_language" - 卑猥な表現。• "chats" - チャット。• "terrorism" - テロリズム。• "free_email" - 無料メール。• "social_networks" - ソーシャルネットワーク。• "owners_notice" - 著作権者からの申し立てによってリストに登録されたWebサイト。• "online_games" - オンラインゲーム。• "anonymizers" - アノニマイザー。• "cryptocurrency_mining_pools" - 仮想通貨マイニングプール。• "jobs" - 求人情報のWebサイト。• "black_list" - ブラックリスト。	文字列または文字列のテーブル
category_not	URLが該当しないカテゴリーのリスト（大文字と小文字は区別されません）。	文字列または文字列のテーブル
無効になったメタメソッド: なし		

フィルターフィールドが指定されていない（値が`nil`である）場合、すべての脅威がフィルターと一致します。複数のフィルターフィールドが指定されている場合、条件は接続詞（論理積）によって結合されます。フィルターフィールドがテーブル（リスト）の場合、オブジェクトは少なくとも1つのテーブル（リスト）の項目と一致する必要があります。

テーブルResponse

このテーブルではHTTPレスポンスヘッダーを指定します。

フィールド	説明	データタイプ
status	HTTPレスポンスコード、またはICAPリクエストにHTTPレスポンスヘッダーが含まれていない場合は <code>nil</code> 。	番号



フィールド	説明	データタイプ
reason	レスポンスコードへのコメント。コメントがない場合はnil。	文字列
content_type	HTTPレスポンスのContent-Typeヘッダーから取得される情報。	テーブル ContentType
field	HTTPレスポンスヘッダーの配列。	HeaderField テーブルの配列
search	正規表現を使用してヘッダーを検索する関数。必須のpatterns引数(つまり、検索パターン、Perl構文(PCRE)の1つ(文字列)または複数(文字列の配列)の正規表現)を受け入れ、使用可能なすべてのヘッダーを検索します。引用符で囲まれた文字列を使用する場合は、スラッシュ文字をエスケープする必要があります。 次のブール値を返します。 <ul style="list-style-type: none"> • true - field.name .. ":" .. field.value.decoded文字列が、少なくとも1つのヘッダーに対して指定した少なくとも1つの正規表現と一致する場合。 • false - field.name .. ":" .. field.value.decoded文字列がどのヘッダーに対しても、どの正規表現とも一致しない場合。 	機能
value	唯一の引数であるヘッダー名(文字列)を要求する関数。指定された名前を持つ最初のヘッダーの値を返します。この名前のヘッダーがない場合はnilを返します。	機能
無効になったメタメソッド: なし		

テーブルBody

このテーブルではHTTPメッセージ本文を指定します。

フィールド	説明	データタイプ
has_threat	1つのオプション引数filter、つまり ThreatFilter テーブルを受け取る関数(引数がない場合は、空のテーブルを使用するのと同じです)。次のブール値を返します。 <ul style="list-style-type: none"> • true - HTTPメッセージ本文に、指定されたfilter条件を満たす脅威が含まれている場合。 • false - メッセージ本文に、指定された条件を満たす脅威が存在しない場合。 	機能
threats	1つのオプション引数filter、つまり ThreatFilter テーブルを受け取る関数(引数がない場合は、空のテーブルを使用するのと同じです)。HTTPメッセージ本文で検出されたすべての脅威を反復処理できる反復子関数を返します。脅威は、 Virus テーブルを使用して指定されます。	機能



フィールド	説明	データタイプ
content_type	HTTPリクエストまたはレスポンスのContent-Typeヘッダーから取得された本文のMIMEタイプに関する情報が含まれます（解析されているメッセージのタイプによって異なります）。	テーブル ContentType
scan_error	<p>本文のスキャンエラー（発生した場合）。それ以外の場合はnil。以下の値を使用できます。</p> <ul style="list-style-type: none">• "path_not_absolute" - 指定されたパスは絶対パスではありません。• "file_not_found" - ファイルが見つかりませんでした。• "file_not_regular" - ファイルは通常のファイルではありません。• "file_not_block_device" - ブロックデバイスではありません。• "name_too_long" - 名前が長すぎます。• "no_access" - アクセスが拒否されました。• "read_error" - 読み取りエラーが発生しました。• "write_error" - 書き込みエラー。• "file_too_large" - ファイルが大きすぎます。• "file_busy" - ファイルは使用中です。• "unpacking_error" - アンパックエラー。• "password_protected" - アーカイブはパスワードで保護されています。• "arch_crc_error" - CRCアーカイブエラー。• "arch_invalid_header" - 無効なアーカイブヘッダー。• "arch_no_memory" - アーカイブを解凍するための十分なメモリがありません。• "arch_incomplete" - 不完全なアーカイブ。• "can_not_be_cured" - ファイルを修復できません。• "packer_level_limit" - 圧縮されたオブジェクトのネスティングレベルの上限を超えました。• "archive_level_limit" - アーカイブのネスティングレベルの上限を超えました。• "mail_level_limit" - メールファイルのネスティングレベルの上限を超えました。• "container_level_limit" - コンテナのネスティングレベルの上限を超えました。• "compression_limit" - 圧縮率の上限を超えました。• "report_size_limit" - レポートサイズの上限を超えました。• "scan_timeout" - スキャンタイムアウトの上限を超えました。	文字列



フィールド	説明	データタイプ
	<ul style="list-style-type: none">"engine_crash" - スキャンエンジンの障害。"engine_hangup" - スキャンエンジンのハングアップ。"engine_error" - スキャンエンジンエラー。"no_license" - アクティブなライセンスが見つかりません。"multiscan_too_late" - マルチスキャンエラー。"curing_limit_reached" - 修復試行の上限を超えました。"non_supported_disk" - サポートされていないディスクタイプ。"unexpected_error" - 予期しないエラー。	
無効になったメタメソッド: なし		

テーブルVirus

このテーブルでは脅威を指定します。

フィールド	説明	データタイプ
name	脅威の種類 (Doctor Webの分類による)	文字列
type	脅威の種類 (Doctor Webの分類による)。以下の値を使用できません。 <ul style="list-style-type: none">"known_virus" - 既知の脅威 (ウイルスデータベースに登録されている脅威)。"virus_modification" - 既知の脅威の亜種。"unknown_virus" - 未知の脅威、疑わしいオブジェクト。"adware" - 広告プログラム。"dialer" - ダイアラープログラム。"joke" - ジョークプログラム。"riskware" - 潜在的に危険なプログラム。"hacktool" - ハッキングツール。	文字列
無効になったメタメソッド: なし		

テーブルThreatFilter

このテーブルでは脅威のフィルターを指定します。フィールドはすべてオプションです。

フィールド	説明	データタイプ
category	脅威が該当するカテゴリーのリスト (大文字と小文字は区別されません)。Virusテーブルのtypeフィールドの説明にあるカテゴリーのリストを参照してください。	文字列または文字列のテーブル



フィールド	説明	データタイプ
category_not	脅威が該当しないカテゴリのリスト(大文字と小文字は区別されません)。	文字列または文字列のテーブル
無効になったメタメソッド: なし		

フィルターフィールドが指定されていない(値が`nil`である)場合、脅威はフィルターと一致します。複数のフィルターフィールドが指定されている場合、条件は接続詞(論理積)によって結合されます。フィルターフィールドがテーブル(リスト)の場合、オブジェクトは少なくとも1つのテーブル(リスト)の項目と一致する必要があります。

使用例:

1. HTTPメッセージで見つかったすべての脅威の名前をログへ書き込む。

```
local dw = require "drweb"

function message_hook(ctx)
  for virus in ctx.body.threats() do
    dw.notice("threat found: " .. virus.name)
  end
  return "pass"
end
```

2. カテゴリフィルターに一致する脅威名と、脅威が検出されたメッセージ部分の名前をログに書き込む。

```
local dw = require "drweb"

function message_hook(ctx)
  for v in ctx.body.threats({category = "known_virus"}) do
    dw.notice("found known virus: " .. v.name)
  end
  return "pass"
end
```

利用可能な補助モジュール

LuaのプログラムスペースでDr.Web for UNIX Internet Gatewaysとやり取りするために、次の特定のモジュールをインポートできます。

モジュール名	機能
drweb	Luaプログラムを起動したDr.Web for UNIX Internet GatewaysコンポーネントのログにLuaプログラムからのメッセージを記録する機能と、Luaプロセスの非同期実行の手段を提供するモジュール
drweb.lookup	Dr.Web LookupDMモジュールを呼び出して、外部ソースからデータを要求するためのツールを提供するモジュール
drweb.regex	文字列と正規表現を一致させるためのインターフェースを提供するモジュール
drweb.config	Dr.Web ICAPD設定パラメータ値を持つテーブルを提供するモジュール



drwebモジュールの内容

1. 機能

このモジュールには、次のような機能があります。

- LuaプログラムからのメッセージをDr.Web for UNIX Internet Gatewaysコンポーネントログに保存する:
 - `log(<level>, <message>)`は<message>文字列をDr.Web for UNIX Internet Gatewaysログに<level>レベル(必要なレベルは、「`debug`」、「`info`」、「`notice`」、「`warning`」、「`error`」を使用して定義します)で書き込みます。
 - `debug(<message>)`は<message>文字列をDr.Web for UNIX Internet Gatewaysログに`DEBUG`レベルで書き込みます。
 - `info(<message>)`は<message>文字列をDr.Web for UNIX Internet Gatewaysログに`INFO`レベルで書き込みます。
 - `notice(<message>)`は<message>文字列をDr.Web for UNIX Internet Gatewaysログに`NOTICE`レベルで書き込みます。
 - `warning(<message>)`は<message>文字列をDr.Web for UNIX Internet Gatewaysログに`WARNING`レベルで書き込みます。
 - `error(<message>)`は<message>文字列をDr.Web for UNIX Internet Gatewaysログに`ERROR`レベルで書き込みます。
- Luaプロセスの同期を管理する:
 - `sleep(<sec.>)`はこのLuaプロセスインスタンスの実行を指定された秒数で一時停止します。
 - `async(<Lua function>[, <argument list>])`は、指定された関数を非同期的に起動し、指定された引数リストに渡します。`async`関数呼び出しはすぐに完了し、戻り値(Futureテーブル)を使用すると、<Lua function>の結果を取得できます。
- [IpAddress](#)テーブルにIPアドレスを追加する:
 - `ip(<address>)`は、IpAddressテーブルの形式で<address>文字列として送信される、IPアドレスを指定します。IPv4またはIPv6アドレスのいずれかを使用できます。
- テキストファイルから外部データをアップロードする:
 - `load_set(<file path>)`は、指定されたテキストファイルのコンテンツから`true`値を含むテーブルを生成します。ファイルから読み取られた文字列はキーとして使用されます。空の文字列と空白を含む文字列は無視されます。
 - `load_array(<file path>)`は、指定されたテキストファイルのコンテンツから文字列の配列を生成します。空の文字列と空白文字のみで構成される文字列は無視され、配列には含まれません。

2. テーブル

- Futureテーブルは、`async`関数を使用して関数を実行した後の保留中の結果を表します。

フィールド	説明	データタイプ
<code>wait</code>	<code>async</code> 関数を使用して開始した関数の結果を返す関数。関数がまだ実行を完了していない場合は、完了を待って結果を返します。 <code>wait</code> が呼び出される前に関数が完了した場合、結果はすぐに返されます。開始された関数が失敗した場合、 <code>wait</code> 呼び出しは同じエラーを生成します。	機能



フィールド	説明	データタイプ
無効になったメタメソッド: なし		

- IpAddressテーブルはIPアドレスを表します。

フィールド	説明	データタイプ
belongs	<p>IpAddressテーブルに保存されているIPアドレスが、指定されたサブネット (IPアドレス範囲) に所属しているかどうかを確認する関数</p> <p>"<IP address>"または "<IP address>/<mask>"のような文字列を唯一の引数として受け取ります。ここで、<IP address>はホストアドレスまたはネットワークアドレス ("127.0.0.1"など)、<mask>はサブネットワークマスク ("255.0.0.0"などのIPアドレスとして、または "8"などの数値形式で指定できます) です。</p> <p>次のブール値を返します。</p> <ul style="list-style-type: none">• trueは、アドレスが指定されたアドレスの少なくとも1つと等しいか、指定されたサブネット (IPアドレスの範囲) の少なくとも1つに属していることを示します。• false - それ以外の場合。	機能
無効になったメタメソッド:		
<ul style="list-style-type: none">• __tostringは、文字列内のIpAddressを変更する関数 (例: "127.0.0.1" (IPv4) または ":::1" (IPv6)) です。• __concatは、IpAddressを文字列に結合する関数です。• __eqは、2つのIpAddressが等しいことを確認する関数です。• __bandは、マスクを適用するための関数 (例: dw.ip('192.168.1.2') & dw.ip('255.255.254.0')) です。		

3. 例

- 非同期的に開始される手順によって生成されるメッセージをログへ書き込む:



```
local dw = require "drweb"

-- This function waits two seconds and returns a string,
-- received as an argument
function out_msg(message)
  dw.sleep(2)
  return message
end

-- "Main" function
function intercept(ctx)
  -- Output of a string at the NOTICE level to the Dr.Web for UNIX Internet
  Gateways log
  dw.notice("Intercept function started.")

  -- An asynchronous start of two copies of the out_msg function
  local f1 = dw.async(out_msg, "Hello,")
  local f2 = dw.async(out_msg, " world!")

  -- Waiting for the completion of the copies of the function
  -- out_msg and output its results to log
  -- the Dr.Web for UNIX Internet Gateways log at the DEBUG level
  dw.log("debug", f1.wait() .. f2.wait())
end
```

- スケジュールされた手順を作成する:

```
local dw = require "drweb"

-- Save the table Future in the future global variable in order
-- to preven the removal by the garbage collector
future = dw.async(function()
  while true do
    -- Everyday, the following message is displayed in the log
    dw.sleep(60 * 60 * 24)
    dw.notice("A brand new day began")
  end
end)
```

- 文字列で表現されたIPアドレスを[IpAddress](#)テーブルに変更する:

```
local dw = require "drweb"

local ipv4 = dw.ip("127.0.0.1")
local ipv6 = dw.ip(":::1")
local mapped = dw.ip("::ffff:127.0.0.1")
```

drweb.lookupモジュールの内容

1. 機能

このモジュールは次の機能を提供します。

- `lookup(<request>, <parameters>)`は、Dr.Web LookupDモジュールを介して利用できる外部スト



レージからデータを要求します。<request>引数は、Dr.Web LookupD設定内のセクション(文字列<type>@<tag>)に対応している必要があります。<parameters>引数は任意で、リクエストを生成するために使用される置換を表します。以下の自動的に許可されるマーカーを使用できます。

- \$u、\$Uは、クライアントコンポーネントによって送信されたユーザー名(user)に自動的に置き換えられます。
- \$d、\$Dは、クライアントコンポーネントによって送信されたドメイン(domain)に自動的に置き換えられます。

これらの引数はテーブルとして設定されます。このテーブルのキーと値は文字列でなければなりません。この関数は、リクエストの結果である文字列の配列を返します。

- check(<checked string>, <request>, <parameters>)は、Dr.Web LookupDモジュールを介して利用できる外部リポジトリで<checked string>が見つかった場合にtrueを返します。引数<request>および<parameters>はlookup関数の引数と同じです(上記を参照)。<checked string>引数は、文字列または__tostringメタメソッドを持つテーブル(つまり、文字列にフォーマットできる)であると想定されます。

2. 例

- LookupD.LDAP.usersデータソースから取得したユーザーのログリストへ書き込む:

```
local dw = require "drweb"
local dwl = require "drweb.lookup"

-- "Main" function
function intercept(ctx)
  -- Writing the string at the NOTICE level to the Dr.Web for UNIX Internet Gateways log
  dw.notice("Intercept function started.")

  -- Writing the request results to the Dr.Web for UNIX Internet Gateways log
  -- to the 'ldap@users' data source
  for _, s in ipairs(dwl.lookup("ldap@users", {user="username"})) do
    dw.notice("Result for request to 'ldap@users': " .. s)
  end
end

end
```

drweb.regexモジュールの内容

1. 機能

このモジュールは次の機能を提供します。

- search(<template>, <text>[, <flags>]) - <text>文字列に<template>正規表現と一致するサブストリングが含まれている場合はtrueを返します。オプションの<flags>パラメータ(整数)は、関数の動作に影響を与える一連のフラグであり、論理和でつなげられます。
- match(<template>, <text>[, <flags>]) - <template>正規表現がそのサブストリングだけでなく<text>ストリング全体と一致しなければならない点を除いてsearchと同じです。

2. 利用可能なフラグ

- ignore_caseはテキストの大文字と小文字を区別しません。

3. 例



```
local rx = require "drweb.regex"

rx.search("te.?t", "some Text") -- false
rx.search("te.?t", "some Text", rx.ignore_case) -- true

rx.match("some.+", "some Text") -- true
```

drweb.configモジュールの内容

1. 機能

このモジュールには関数はありません。

2. 利用可能なテーブル

このモジュールは、次のフィールドを持つテーブルを提供します。

フィールド	説明	データタイプ
whitelist	Whitelist設定パラメータの値。	文字列の配列
blacklist	Blacklist設定パラメータの値。	文字列の配列
adlist	Adlist設定パラメータの値。	文字列の配列
block_url_categories	ブロックされるURLカテゴリーのリスト(Yesに設定されたBlock*パラメータ値に基づく)。	文字列の配列
block_threats	ブロックされる脅威カテゴリーのリスト(Yesに設定されたBlock*パラメータ値に基づく)。	文字列の配列
block_unchecked	BlockUnchecked設定パラメータの値。	論理

無効になったメタメソッド: なし

3. 例

```
local cfg = require "drweb.config"

function message_hook(ctx)

  -- Block messages containing threats
  -- from the list of threats to be blocked
  if ctx.body.has_threat{category = cfg.block_threats} then
    return "block"
  end

  -- To permit access to all other resources
  return "pass"

end
```



SpIDer Gate



このコンポーネントはGNU/Linux OSのディストリビューションにのみ含まれています。

ネットワークトラフィックとURLを監視するコンポーネントSpIDer Gateは、データ(ネットワークからローカルコンピューター、ローカルホストからネットワークにダウンロードされたデータ)の脅威を検査し、望ましくないカテゴリーに含まれるWebリソースや、管理者によって定義されたブラックリストに含まれるネットワークホストとの接続を防止します。

コンポーネント設定では、スキャン対象のプロトコルの種類を指定できます。

このコンポーネントは、URLがいずれかのカテゴリー(HTTP/HTTPSプロトコルを利用する接続のスキャンに使用される)に属しているかどうかを確認するために、Doctor Webの更新サーバーから定期的に更新されるWebリソースカテゴリーのデータベースを使用するだけでなく、Dr.Web Cloudサービスの参照も行います。Doctor Webは、以下のWebリソースカテゴリーを追跡します。

- *InfectionSource* - 悪意のあるソフトウェアを含むWebサイト(「感染源」)。
- *NotRecommended* - アクセスすることが推奨されない不正なWebサイト(「ソーシャルエンジニアリング」を使用しているもの)。
- *AdultContent* - ポルノまたはエロティックなコンテンツ、出会い系サイトなどを含むWebサイト。
- *Violence* - 暴力行為を助長するWebサイトや、さまざまな死亡事故などに関するコンテンツを含むWebサイト。
- *Weapons* - 武器および爆発物に関するWebサイトや、それらの製造に関する情報を提供しているWebサイト。
- *Gambling* - 勝負事、カジノ、オークションなどのオンラインゲームへのアクセスを提供するWebサイト(賭けサイトなどを含む)。
- *Drugs* - 麻薬の使用、製造または流通などを促進するWebサイト。
- *ObsceneLanguage* - (タイトルや記事などに)卑猥な表現を含むWebサイト。
- *Chats* - テキストメッセージのリアルタイム送信を提供するWebサイト。
- *Terrorism* - 攻撃的なプロパガンダ、またはテロ攻撃などに関する内容を含むWebサイト。
- *FreeEmail* - メール無料登録を提供するWebサイト。
- *SocialNetworks* - さまざまなソーシャルネットワークサービス: 一般、仕事、企業、興味、テーマ別出会い系サイト。
- *DueToCopyrightNotice* - 一部の著作物(映画、音楽など)の著作権者によって定義されるWebサイト。
- *OnlineGames* - インターネットへの常時接続を使用してゲームへのアクセスを提供するWebサイト。
- *Anonymizers* - ユーザーが個人情報を隠し、ブロックされたWebリソースにアクセスすることを可能にするWebサイト。
- *CryptocurrencyMiningPool* - 仮想通貨マイニングのための一般的なサービスへのアクセスを提供するWebサイト。
- *Jobs* - 求人検索Webサイト。

システム管理者は、ホストが属するカテゴリーに基づいて、望ましくないホストへのアクセスを設定できます。またユーザーは、特定のホストへのアクセスをブロックするために独自のブラックリストを設定したり、アクセスを許可す



のためにホワイトリストを設定したりすることもできます。ホワイトリストのホストへのアクセスは、それらが望ましくないカテゴリに属する場合でも許可されます。ローカルのブラックリストとWebリソースのカテゴリのデータベースにURLに関する情報がない場合、コンポーネントはDr.Web Cloudサービスを参照して、他のDr.Web製品から受信するこうしたURLに悪意があるかどうかの情報をリアルタイムで検査できます。



同一のWebサイトは、複数のカテゴリに同時に所属することができます。そのようなWebサイトへのアクセスは、不要なカテゴリのいずれに属する場合もブロックされます。

Webサイトがホワイトリストに含まれる場合でも、データ（Webサイトから送信およびダウンロードされたもの）に脅威が含まれているかどうかはスキャンされます。

HTTPプロトコルを介して転送されるファイルのスキャンの負荷が高まると、[Dr.Web Network Checker](#)コンポーネントが利用できるファイル記述子の数が減少するため、スキャンに問題が生じる場合があります。この場合、Dr.Web for UNIX Internet Gatewaysに利用できるファイル記述子の[制限数を増やす](#)必要があります。

Dr.Web for UNIX Internet Gatewaysは、社内のサーバー（公開されているWebサーバーなど）と外部ネットワークであるインターネットとの間に「壁」を作るために組織内で使用できます。デフォルトで、[Dr.Web ICAPD](#)コンポーネントがユーザーアクセスを制御する機能を実行するためです。このコンポーネントは、ローカルネットワークからインターネットへのアクセスを提供するプロキシサーバーと連携して機能します。

動作原理

SpIDer Gateコンポーネントは、ユーザーアプリケーションによって確立されたネットワーク接続を監視します。このコンポーネントは、クライアントアプリケーションが接続しようとしているサーバーが、設定で望ましくないと指定されているWebリソースカテゴリのいずれかに属するかどうかを検査します。さらにこのコンポーネントは、Dr.Web Cloudを参照してURLを検査できます。URLが望ましくないカテゴリ（Dr.Web Cloudのリクエストによって返されたものを含む）に属する場合や、システム管理者によって定義されたブラックリストに属する場合、接続は中断され、アクセスが許可されていないというメッセージが含まれるHTMLページが表示されます（HTTP/HTTPS接続の場合）。HTMLページは、コンポーネントに付属するテンプレートに従ってSpIDer Gateによって生成されます。このページには、リクエストされたリソースにアクセスできないという通知と、ブロックに関する詳細が表示されます。SpIDer Gateがブロックする必要がある脅威を見つけた場合にも同様のページが表示され、クライアントに返されます。接続にHTTP(S)とは異なるプロトコルが使用されている場合、コンポーネントはこのサーバーとの接続を確立するための許可のみをスキャンします。

補助コンポーネント[Dr.Web Firewall for Linux](#)は、クライアントアプリケーションによって確立されたりリモートサーバーとの接続をリダイレクトします。このコンポーネントはGNU/LinuxシステムコンポーネントのNetFilterルールの動的管理を実行します。

Dr.Web for UNIX Internet Gateways内では、クライアントアプリケーションは会社の保護されたサーバーリソースになります（公開されているWebサーバーなど）。デフォルトで、[Dr.Web ICAPD](#)コンポーネントがローカルネットワークユーザーのインターネットへのアクセスを管理する機能を実行するためです。このコンポーネントは、ローカルネットワークからインターネットへのアクセスを提供するプロキシサーバーと連携して動作します。

[Dr.Web Updater](#)コンポーネントは、Doctor Web更新サーバーからWebリソースカテゴリのデータベースを定期的かつ自動的に更新するために使用されます。同じコンポーネントは、[Dr.Web Scanning Engine](#)スキャンエンジン用のウイルスデータベースの更新にも使用されます。[Dr.Web CloudD](#)コンポーネントはDr.Web Cloudサービスの参照に使用されます（クラウドサービスの使用は付録[共通設定](#)で設定され、必要に応じて無効にでき



ます)。転送されたデータを検査するために、SpIDer Gateは[Dr.Web Network Checker](#)コンポーネントを使用します。后者では、[Dr.Web Scanning Engine](#)スキャンエンジンを介してスキャンが開始されます。

コマンドライン引数

SpIDer Gateを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-gated [<parameters>]
```

SpIDer Gateは次のオプションを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了します。 短縮形：-h 引数：なし
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了します。 短縮形：-v 引数：なし

例：

```
$ /opt/drweb.com/bin/drweb-gated --help
```

このコマンドはSpIDer Gateに関する簡単なヘルプ情報を出力します。

スタートアップノート

このコンポーネントは、自律モードで(他のコンポーネントから自律的に)OSのコマンドラインから直接起動することはできません。必要に応じて[Dr.Web ConfigD](#)設定デーモンによって自動的に起動されます。コンポーネントの動作を管理するには、Dr.Web for UNIX Internet Gateways用のコマンドラインベース管理ツール[Dr.Web Ctl](#)を使用できます(これはdrweb-ctlコマンドを使用して呼び出されます)。



コマンドラインから製品のこのコンポーネントに関するドキュメントを取得するには、`man 1 drweb-gated`コマンドを使用します。

設定パラメータ

このコンポーネントは、Dr.Web for UNIX Internet Gatewaysの統合された[設定ファイル](#)の[GateD]セクションで指定されている設定パラメータを使用します。



セクションには以下のパラメータが含まれています。

パラメータ	説明
LogLevel <i>{logging level}</i>	コンポーネントの ロギングレベル 。 パラメータの値が指定されていない場合は、[Root] セクション のDefaultLogLevelパラメータの値が使用されます。 デフォルト値 : Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値 : Auto
ExePath <i>{path to file}</i>	コンポーネントの実行パス。 デフォルト値 : <opt_dir>/bin/drweb-gated <ul style="list-style-type: none">• GNU/Linuxの場合 : /opt/drweb.com/bin/drweb-gated• FreeBSDの場合 : /usr/local/libexec/drweb.com/bin/drweb-gated
RunAsUser <i>{UID user name}</i>	その権限によりコンポーネントを実行するユーザーの名前。このユーザー名は、ユーザーのUIDまたはユーザーのログインとして指定できます。ユーザー名が数字で構成されている場合(つまりUIDに似ている場合)は、「name:」というプレフィックスを付けて指定します。たとえば、RunAsUser = name:123456です。 ユーザー名が指定されていない場合、コンポーネント動作は、開始後に発生するエラーによって終了します。 デフォルト値 : drweb
IdleTimeLimit <i>{time interval}</i>	コンポーネントの最大アイドル時間。指定された時間が経過すると、コンポーネントはシャットダウンします。 指定可能な値 : 10秒 (10s) から30日 (30d) まで。 None値が設定されている場合、コンポーネントは永続的に機能します。コンポーネントがアイドル状態になると、SIGTERMシグナルは送信されません。 デフォルト値 : 30s
TemplatesDir <i>{path to directory}</i>	Webリソースをブロックしたときに送信されるHTML通知のテンプレートを含むディレクトリへのパス。 デフォルト値 : <var_dir>/templates/gated <ul style="list-style-type: none">• GNU/Linuxの場合 : /var/opt/drweb.com/templates/gated• FreeBSDの場合 : /var/drweb.com/templates/gated
CaPath <i>{path}</i>	信頼できるルート証明書のシステムリストを含むディレクトリまたはファイルへのパス。 デフォルト値 : 信頼できる証明書のリストへのパス。パスは、お使いのGNU/Linuxディストリビューションに依存します。 <ul style="list-style-type: none">• Astra Linux、Debian、Linux Mint、SUSE Linux、Ubuntuの場合、通常はパス/etc/ssl/certs/です。



パラメータ	説明
	<ul style="list-style-type: none">• CentOSとFedoraの場合はパス/etc/pki/tls/certs/ca-bundle.crtです。• 他のディストリビューションでは、コマンド<code>openssl version -d</code>の実行結果によってパスを定義できます。• コマンドが使用できない場合、またはOSディストリビューションを特定できない場合は、値/etc/ssl/certs/が使用されます。



接続スキャンの設定を変更しても、変更を加える前にアプリケーションによってすでに確立されている接続のスキャンには影響しません。

補助コンポーネントDr.Web Firewall for Linuxの[設定](#)で、トラフィックモニタリングのより具体的なパラメータを指定します。

Dr.Web Firewall for Linux



このコンポーネントはGNU/Linux OSのディストリビューションにのみ含まれています。

コンポーネントを正しく動作させるため、以下のオプションを指定してOSカーネルが構築されている必要があります。

- `CONFIG_NETLINK_DIAG, CONFIG_INET_TCP_DIAG;`
- `CONFIG_NF_CONNTRACK_IPV4, CONFIG_NF_CONNTRACK_IPV6, CONFIG_NF_CONNTRACK_EVENTS;`
- `CONFIG_NETFILTER_NETLINK_QUEUE, CONFIG_NETFILTER_NETLINK_QUEUE_CT, CONFIG_NETFILTER_XT_MARK.`

必要なオプションの組み合わせは、使用するGNU/Linuxのディストリビューションキットによって異なります。

Dr.Web Firewall for Linuxは補助コンポーネントです。SpIDer Gatelに対して接続マネージャーの役割を果たします。Dr.Web Firewall for Linuxが機能することで、ホスト接続がSpIDer Gateを通過し、接続トラフィックが監視されます。

動作原理

このセクションの内容:

- [概要](#)
- [接続監視のメカニズム](#)
- [接続監視の順序](#)

概要

SpIDer GatelはDr.Web Firewall for Linuxコンポーネントの働きにより正常に動作します。このコンポーネントは、NetFilter(GNU/Linux OSコンポーネント)用に調整されたルーティングルールを解析し、確立された接続が、クライアントアプリケーションとリモートサーバー間の中間の機能(プロキシ)を実行するSpIDer Gatelにリダイレクトされるように修正します。

Dr.Web Firewall for Linuxは、トランジット接続だけでなく、送信と受信のリダイレクトのルールを別々に管理できます。バイパスまたはリダイレクトのルールを正確に設定するには、コンポーネントではLuaで書かれたスクリプトだけでなく設定に組み込まれたルールを使うことができます。

接続監視のメカニズム

接続を監視するために、Dr.Web Firewall for Linuxはルーティングポリシーのデータベース(`man ip: ip route, ip rule`参照)とNetFilterシステムコンポーネントの`nf_conntrack`インターフェースで指定されたルーティングテーブルを使用します。監視された接続と転送されたパケットには、Dr.Web Firewall for LinuxがNetFilterのチェーンのさまざまな段階で接続をリダイレクトし、転送されたパケットを正しく処理できるようにするビットマークが付けられます(詳細は`man iptables`を参照)。



iptablesルールのアクション

Dr.Web Firewall for Linuxは、iptablesルールで次のアクションを使用します。

- **MARK**: このアクションにより、Dr.Web Firewall for Linuxは指定された数字マークをパケットに設定できます。
- **CONNMARK**: このアクションにより、Dr.Web Firewall for Linuxは指定された数字マークを接続に設定できます。
- **TPROXY**: このアクションにより、Dr.Web Firewall for Linuxは、パケットのコンテンツを変更することなく、**PREROUTING** NetFilterチェーンから指定されたネットワークソケット (<IP address>: <port>) にパケットをリダイレクトできます。このアクションを使用すると、Dr.Web Firewall for Linuxは接続の最初の宛先アドレスを特定できます。
- **NFQUEUE**: このアクションにより、エンジンのネットワークスタックから、スキャンのためにカーネル空間外で動作するプロセスにパケットを送信できます。したがって、Dr.Web Firewall for Linuxは、特殊な *Netlink* ソケットを介して、指定した番号のキュー **NFQUEUE** に接続し、処理で判定するために必要なパケットを入手します (Dr.Web Firewall for Linuxは、NetFilterに、**DROP**: ドロップ、**ACCEPT**: 許可、**REPEAT**: 繰り返しのいずれかの判定を伝える必要があります)。

パケットと接続のマーク

パケットをマークするため、Dr.Web Firewall for Linuxは、パケットおよび接続マークで使用可能な32ビットのうち次の3つを使用します。

- **LDM**ビット (*Local Delivery Mark*)。マークにこのビットがあるパケットは、使用しているルーティングルールに基づいてローカルホストに送信されます。
- **CPM**ビット (*Client Packets Mark*)。クライアント (接続開始側) とプロキシ (Dr.Web Firewall for Linuxなど) の間の接続を示します。
- **SPM**ビット (*Server Packets Mark*)。プロキシ (Dr.Web Firewall for Linuxなど) とサーバー (接続受信側) の間の接続を示します。

LDM、CPM、SPMビットは、ルーティング接続を実行する他のアプリケーションがパケットをマークするために使用していない任意のさまざまなビットにすることができます。デフォルトでは、Dr.Web Firewall for Linuxは適切な (他のアプリケーションでは使用されていない) ビットを自動的に選択します。

ルートとルーティングポリシー (ip rule、ip route)

Dr.Web Firewall for Linuxを (あらゆる接続スキャンモードで) 正しく動作させるには、100番のルーティングテーブルを使用する `ip rule` ルーティングポリシーをシステムに設定する必要があります。

```
from all fwmark <LDM>/<LDM> lookup 100
```

次のルートをテーブルに追加する必要があります。

```
local default dev lo scope host
```

このルーティングポリシーは、マークにLDMビットが入っているパケットが常にローカルホストに送信されることを保証します。



それ以降、 XXX ビットの $\langle XXX \rangle$ 文字列は、 2^N (N はパケットマーク内の XXX ビットの序数)に等しい16進値になります。たとえば、最小(ゼロ)ビットがLDMビットとして選択されている場合は、 $\langle LDM \rangle = 2^0 = 0x1$ になります。

NetFilter (iptables) のルール

Dr.Web Firewall for Linuxを(あらゆる接続スキャンモードで)正しく動作させるには、次の6つのルール (iptables-save出力コマンド形式で表示)がNetFilterシステムコンポーネントの該当するチェーンのnatテーブルとmangleテーブルに存在する必要があります。

```
*nat

-A POSTROUTING -o lo -m comment --comment drweb-firewall -m mark --mark
<LDM>/<LDM> -j ACCEPT

*mangle

-A PREROUTING -m comment --comment drweb-firewall -m mark --mark
0x0/<CPM+SPM> -m connmark --mark <SPM>/<CPM+SPM> -j MARK --set-xmark
<LDM>/<LDM>

-A PREROUTING -p tcp -m comment --comment drweb-firewall -m mark ! --mark
<CPM+SPM>/<CPM+SPM> -m connmark --mark <CPM>/<CPM+SPM> -j TPROXY --on-port
<port> --on-ip <IP-address> --tproxy-mark <LDM>/<LDM>

-A OUTPUT -m comment --comment drweb-firewall -m mark --mark
<CPM>/<CPM+SPM> -j CONNMARK --set-xmark <CPM>/0xffffffff

-A OUTPUT -m comment --comment drweb-firewall -m mark --mark
<SPM>/<CPM+SPM> -j CONNMARK --set-xmark <SPM>/0xffffffff

-A OUTPUT -m comment --comment drweb-firewall -m mark --mark 0x0/<CPM+SPM>
-m connmark ! --mark 0x0/<CPM+SPM> -j MARK --set-xmark <LDM>/<LDM>
```



以下の説明では、0~5の番号がこれらのルールに割り当てられています(文書に記載されている順序で)。式 $\langle X+Y \rangle$ は、それぞれの数 X と Y のビット数「OR」(合計)を意味します。

ルール番号2のパラメータ $\langle IP\ address \rangle$ と $\langle port \rangle$ は、Dr.Web Firewall for Linuxが監視された接続を管理するネットワークソケットを示します。

さらに、Dr.Web Firewall for Linux設定で監視接続モード(送信、受信、トランジット)を有効にする場合は、次の追加ルールが該当するチェーンのmangleテーブル(OUTPUT、INPUT、FORWARD)に存在する必要があります。

- 送信(OUTPUT)接続を監視するには:

```
-A OUTPUT -p tcp -m comment --comment drweb-firewall -m tcp --tcp-flags
SYN,ACK SYN -m mark --mark 0x0/<CPM+SPM> -j NFQUEUE --queue-num <ONum> --
queue-bypass
```

- 受信(INPUT)接続を監視するには:



```
-A INPUT -p tcp -m comment --comment drweb-firewall -m tcp --tcp-flags SYN,ACK SYN -m mark --mark 0x0/<CPM+SPM> -j NFQUEUE --queue-num <INum> --queue-bypass
```

- トランジット(*FORWARD*) 接続を監視するには:

```
-A FORWARD -p tcp -m comment --comment drweb-firewall -m tcp --tcp-flags SYN,ACK SYN -m mark --mark 0x0/<CPM+SPM> -j NFQUEUE --queue-num <FNum> --queue-bypass
```



以下の説明では、6、7、8の番号がこれらのルールに割り当てられています（文書に記載されている順序で）。

ここで、<ONum>、<INum>、<FNum>は、Dr.Web Firewall for Linuxが対応する接続のインストールを示すパケット（SYNフラグが設定されているがACKフラグは含まれていないパケット）を待機しているNFQUEUE内のキューの数です。

接続監視の順序

ルール6、7、8のいずれかに従って、対応する方向の新しいネットワーク接続を示すパケットは、CPMとSPMのどちらのビットでもマークされていない場合、NetFilterによって該当するNFQUEUEキューに入れられます。ここでパケットは、*nf_conntrack*インターフェースを介してDr.Web Firewall for Linuxによって読み取られます。ルール3と4は、接続を監視済みとしてマークします。つまり、接続マークに接続方向が設定されていることを示すビットがあります。このビット番号は、パケットマークのビット番号と一致します。その結果、ルール1、2、5に従って、この接続を介して送信されたパケットはDr.Web Firewall for Linuxによって配信されます。ルール0がnatテーブルのPOSTROUTINGチェーンの最上部に追加されるため、NATが設定されている場合、マークされたパケットのアドレスは送信されません（Dr.Web Firewall for Linuxの監視および接続処理ロジックに干渉するため）。

パケットがいずれかのNFQUEUEキューに現れると、Dr.Web Firewall for Linuxは、NetFilterで誤ったルールが設定されている場合に備えて、パケットの基本的な処理を実行します。次に、Dr.Web Firewall for Linuxは、ルール4に従い、それ自体の名前と、PSCとマークされたソケットを使用してサーバーへの接続を試みます。ローカル配信のルール5は適用されません。パケットはSPMでマークされており、このルールは<CPM + SPM>でマークされたパケットにのみ適用できるためです。

- サーバーへの接続が失敗した場合、Dr.Web Firewall for Linuxは、RSTビットを含むクライアントパケットを生成し、<IP address>:<port>のペアをリクエストされたサーバーのネットワークソケットのアドレスに置き換えます。DROP判定もNFQUEUEに送信されます。RSTビットを含むパケットの送信に使用されるソケットは<CPM+SPM>としてマークされているため、上記のルールはどれも適用されず、パケットは通常のルーティングルールに従ってクライアントに配信されます。
- リモートサーバーへの接続が成功した場合、Dr.Web Firewall for Linuxは、監視したSYNパケットをコピーし、<LDM+CPM>とマークされたソケットから再送信して、パケットをローカルネットワークソケットにリダイレクトします。LDMビットが設定されているため、指定したルーティングルールに従って出カインターフェースを選択すると、パケットは*looback*インターフェースに追加されます。その後、NetFilter PREROUTINGチェーンに追加され、そこでルール2が適用されます。したがって、パケットは変更されることなくネットワークソケットDr.Web Firewall for Linuxにリダイレクトされます。この機能により、Dr.Web Firewall for Linuxは接続アドレスの4つの要素すべて（パケット送信者のIPアドレスとポート、パケット受信者のIPアドレスとポート）を保存できます。

Dr.Web Firewall for Linuxがルール2に従って監視した接続を受信するネットワークソケットの場合、IP_TRANSPARENTオプションと<LDM+CPM>マークが設定され、このソケットからDr.Web Firewall for

Linuxによって送信されたパケットが*NFQUEUE*キューに分類されないようにします。クライアントが接続すると、保存されている4要素のアドレス(パケット送信者のIPアドレスとポート、パケット受信者のIPアドレスとポート)を使用して、ペアのソケットが検索されます。クライアントとサーバーの接続が確立されると、Luaの手順とDr.Web Firewall for Linuxの設定で指定されたスキャンルールに従ってスキャンされます。スキャンが成功し、接続が安定している場合は、クライアント側とサーバー側を接続する関連ソケットのペアが転送データの解析のためにSpIDer Gateコンポーネントに転送されます。それに続くクライアントとサーバー間の対話は、メディエーターのSpIDer Gateを介して確立されます。Dr.Web Firewall for Linuxは、クライアント側とサーバー側に関連付けられたソケットペアに加えて、確立された接続をスキャンするためのパラメータとルールをSpIDer Gateに送信します。

Dr.Web Firewall for Linux動作の概略図を以下に示します。

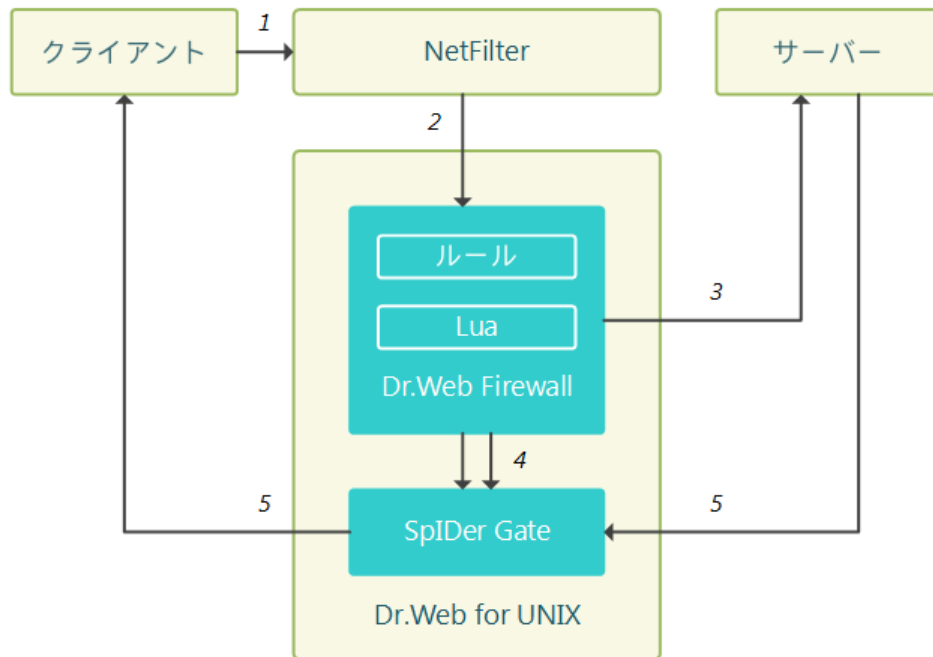


図 12. コンポーネントの動作図

以下の接続処理のステップには番号が付いています。

1. クライアントがサーバーへの接続を試みます。
2. ルーティングルールに従って、NetFilterの接続をDr.Web Firewall for Linuxにリダイレクトします。
3. Dr.Web Firewall for Linuxは、クライアントの名前と接続スキャンを使用して、サーバーへの接続を試みます。
4. 接続のクライアント側とサーバー側、接続処理用のSpIDer Gate、およびスキャンの設定とルールに関連するソケットペアを送信します。
5. メディエーターとしてSpIDer Gateを介し、サーバーとクライアント間でデータ交換を行います。



Dr.Web Firewall for Linuxを正しく動作させるためには、ルーティングテーブルに正しい数のビットマーク、*NFQUEUE*キュー、接続監視用のネットワークソケットアドレスを使用するためのルールが必要です。デフォルト設定では、コンポーネントは必要なルール設定を自動的に実行します。設定で接続の自動設定が無効になっている場合、コンポーネントを起動するときに必要なルールを手動で入力する必要があります。



コマンドライン引数

Dr.Web Firewall for Linuxを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-firewall [<options>]
```

Dr.Web Firewall for Linuxは次のオプションを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了します。 短縮形：-h 引数：なし
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了します。 短縮形：-v 引数：なし

例：

```
$ /opt/drweb.com/bin/drweb-firewall --help
```

このコマンドはDr.Web Firewall for Linuxに関する簡単なヘルプ情報を出力します。

スタートアップノート

このコンポーネントは、自律モードで(他のコンポーネントから自律的に)OSのコマンドラインから直接起動することはできません。必要に応じて[Dr.Web ConfigD](#)設定デーモンによって自動的に起動されます。コンポーネントの動作を管理するには、Dr.Web for UNIX Internet Gateways用のコマンドラインベース管理ツール[Dr.Web Ctl](#)を使用できます(これはdrweb-ctlコマンドを使用して呼び出されます)。



コマンドラインから製品のこのコンポーネントに関するドキュメントを取得するには、`man 1 drweb-firewall`コマンドを使用します。

設定パラメータ

このコンポーネントは、Dr.Web for UNIX Internet Gatewaysの統合された[設定ファイル](#)の[LinuxFirewall]セクションで指定されている設定パラメータを使用します。

- [コンポーネントパラメータ](#)
- [トラフィックモニタリングとアクセスブロックのルール](#)



コンポーネントパラメータ

セクションには以下のパラメータが含まれています。

パラメータ	説明
LogLevel <i>{logging level}</i>	コンポーネントの ロギングレベル 。 パラメータの値が指定されていない場合は、[Root] セクション のDefaultLogLevelパラメータの値が使用され ます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行パス。 デフォルト値: <opt_dir>/bin/drweb-firewall <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-firewall• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-firewall
XtablesLockPath <i>{path to file}</i>	iptables (NetFilter) テーブルブロックファイルへのパス。パラメータ値が指定されていない場合は、/run/xtables.lock と/var/run/xtables.lockパスが検査されます。指定されたパスまたはデフォルトのパスにファイルが見つからない場合は、コンポーネントを起動したときにエラーが発生 します。 デフォルト値: (指定なし)
InspectFtp <i>{On / Off}</i>	FTPプロトコルを介して転送されたデータをスキャンします。 データはルールに従ってスキャンされます (下記参照)。 デフォルト値: On
InspectHttp <i>{On / Off}</i>	HTTPプロトコルを介して転送されたデータをスキャン します。 データはルールに従ってスキャンされます (下記参照)。 デフォルト値: On
InspectSmtpt <i>{On / Off}</i>	SMTPプロトコルを介して転送されたデータをスキャン します (インストールされている場合は、Dr.Web MailDコン ポーネントが使用されます)。 実際のデータスキャンは、指定されたスキャンルールに従 って実行されます (下記参照)。



パラメータ	説明
	デフォルト値 : On
InspectPop3 {On / Off}	POP3プロトコルを介して転送されたデータをスキャンします (インストールされている場合は、Dr.Web MailDコンポーネントが使用されます)。 実際のデータスキャンは、指定されたスキャンルールに従って実行されます (下記参照)。 デフォルト値 : On
InspectImap {On / Off}	IMAPプロトコルを介して転送されたデータをスキャンします (インストールされている場合は、Dr.Web MailDコンポーネントが使用されます)。 実際のデータスキャンは、指定されたスキャンルールに従って実行されます (下記参照)。 デフォルト値 : On
AutoconfigureIptables {Yes / No}	iptablesインターフェースを介してNetFilterシステムコンポーネントを設定するためのルール。 使用可能な値 : <ul style="list-style-type: none">• Yes - コンポーネントを起動するときにNetFilterのルールを設定し、動作を自動的に終了するときにルールを削除します (推奨)。• No - ルールを自動的に設定しません。必要なルールは、コンポーネントを起動する前に管理者が手動で追加し、動作が完了した後に削除する必要があります。 <div style="border: 1px solid #ccc; background-color: #fff9c4; padding: 10px; margin: 10px 0;"> iptablesのルールの自動設定が許可されていない場合は、iptablesに必要なルールがコンポーネント動作開始前に利用できるようなっている必要があります。</div> デフォルト値 : Yes
AutoconfigureRouting {Yes / No}	ip routeとip ruleのルーティングルールとポリシーの設定モード。 使用可能な値 : <ul style="list-style-type: none">• Yes - コンポーネントを起動するときにip routeとip ruleのルーティングルールとポリシーを設定し、動作を自動的に終了するときにルーティングルールとポリシーを削除します (推奨)。• No - ルールを自動的に設定しません。必要なルールは、コンポーネントを起動する前に管理者が手動で追加し、動作が完了した後に削除します。



パラメータ	説明
	<div data-bbox="826 264 1449 479" style="border: 1px solid #ccc; background-color: #fff9c4; padding: 10px;"> ルーティングルールとポリシーの自動設定が許可されていない場合は、<code>ip route</code>と<code>ip rule</code>に必要なルールがコンポーネント動作開始前に利用できるようなっている必要があります。</div> <p>デフォルト値 : Yes</p>
LocalDeliveryMark <i>{integer / Auto}</i>	<p>接続を監視するためにDr.Web Firewall for Linuxネットワークソケット (TproxyListenAddressパラメータで指定、下記参照) にリダイレクトされるパケットの <LDM>マーク。</p> <p>使用可能な値 :</p> <ul style="list-style-type: none">• <integer> - パケットの <LDM>マーク。2^Nに等しく、Mがパケット内のLDMビット数の場合、0 ≤ N ≤ 31。• Auto - Dr.Web Firewall for Linuxはパケットマークの適切なビット数を自動的に選択できます (推奨)。 <div data-bbox="826 943 1449 1406" style="border: 1px solid #ccc; background-color: #fff9c4; padding: 10px;"> <LDM>番号を手動で割り当てるときは、(NetFilter経由を含む) ルート接続とパケットを管理する他のアプリケーションが、パケットマークで対応するビット数を使用していないことを確認してください。無効な値を指定した場合、コンポーネントの起動は失敗します。</div> <p>AutoconfigureIptables = No、AutoconfigureRouting = Noの場合、指定された <LDM>番号は、手動で追加する必要があるルーティングルールで使用してください。</p> <p>デフォルト値 : Auto</p>
ClientPacketsMark <i>{integer / Auto}</i>	<p>接続を開始するクライアントとDr.Web Firewall for Linuxの間で転送されるパケットの <CPM>マーク。</p> <p>使用可能な値 :</p> <ul style="list-style-type: none">• <integer> - パケットの <CPM>マーク。2^Nに等しく、Mがパケット内のCPMビット数の場合、0 ≤ N ≤ 31。• Auto - Dr.Web Firewall for Linuxはパケットマークの適切なビット数を自動的に選択できます (推奨)。



パラメータ	説明
	<div data-bbox="826 264 1449 701" style="background-color: #fff9c4; padding: 10px;"><p><CPM>番号を手動で割り当てるときは、(NetFilter経由を含む)ルート接続とパケットを管理する他のアプリケーションが、パケットマークで、対応するビット数を使用していないことを確認してください。無効な値を指定した場合、コンポーネントの起動は失敗します。</p><p>AutoconfigureIptables = Noの場合、指定された<CPM>番号は、手動で追加する必要があるルーティングルールで使用する必要があります。</p></div> <p>デフォルト値 : Auto</p>
ServerPacketsMark <i>{integer / Auto}</i>	<p>Dr.Web Firewall for Linuxと接続を受信するサーバーの間で転送されるパケットの<SPM>マーク。</p> <p>使用可能な値 :</p> <ul style="list-style-type: none">• <integer> - パケットの<SPM>マーク。2^Nに等しく、Nがパケット内のSPMビット数の場合、0 ≤ N ≤ 31。• Auto - Dr.Web Firewall for Linuxはパケットマークの適切なビット数を自動的に選択できます(推奨)。 <div data-bbox="826 1099 1449 1563" style="background-color: #fff9c4; padding: 10px;"><p><SPM>番号を手動で割り当てるときは、(NetFilter経由を含む)ルート接続とパケットを管理する他のアプリケーションが、パケットマークで対応するビット数を使用していないことを確認してください。無効な値を指定した場合、コンポーネントの起動は失敗します。</p><p>AutoconfigureIptables = No、AutoconfigureRouting = Noの場合、指定された<SPM>番号は、手動で追加する必要があるルーティングルールで使用してください。</p></div> <p>デフォルト値 : Auto</p>
TproxyListenAddress <i>{network socket}</i>	<p>Dr.Web Firewall for Linuxが監視した接続を受信するネットワークソケット (<IP address>:<port>)。ポート0を指定すると、システムによって自動的に選択されます。</p>



パラメータ	説明
	<div data-bbox="826 264 1449 638" style="background-color: #fff9c4; padding: 10px;"> 該当するソケットが他のアプリケーションによって使用されていないことを確認する必要があります。無効な値を指定した場合、コンポーネントの起動は失敗します。 AutoconfigureIptables = Noの場合、指定されたIPアドレスとポートは、手動で追加する必要があるルーターティングルールで使用してください。</div> <p data-bbox="790 667 1125 696">デフォルト値 : 127.0.0.1:0</p>
OutputDivertEnable {Yes / No}	<p data-bbox="790 723 1444 817">受信接続(つまりローカルホストに接続があるリモートホストのアプリケーションによって開始された接続)の監視モードを有効/無効にします。</p> <p data-bbox="790 853 981 882">使用可能な値 :</p> <ul data-bbox="790 907 1324 981" style="list-style-type: none">• Yes - 送信接続の監視と処理を行います。• No - 送信接続の監視と処理は行いません。 <div data-bbox="826 1003 1449 1211" style="background-color: #fff9c4; padding: 10px;"> この設定は、AutoconfigureIptables = Noの場合に、手動で追加または削除されるルーターティングルール番号5を追加または削除します。</div> <p data-bbox="790 1240 981 1270">デフォルト値 : No</p>
OutputDivertNfqueueNumber {integer / Auto}	<p data-bbox="790 1301 1444 1361">Dr.Web Firewall for Linuxが、送信接続を開始するSYNパッケージを取得するキュー番号 <i>NFQUEUE</i></p> <p data-bbox="790 1397 981 1426">使用可能な値 :</p> <ul data-bbox="790 1451 1444 1592" style="list-style-type: none">• <integer> - <i>NFQUEUE</i>で監視された送信接続のSYNパッケージを監視するためのキュー番号 <ONum>• Auto - Dr.Web Firewall for Linuxは適切なキュー番号を自動的に選択できます(推奨)。





パラメータ	説明
	<div data-bbox="826 264 1449 701" style="background-color: #fff9c4; padding: 10px;"> <ONum>番号を手動で割り当てるときは、(NetFilterルール経由を含む)接続とパケットを管理する他のアプリケーションが、相応するキュー番号を使用していないことを確認してください。無効な値を指定した場合、コンポーネントの起動は失敗します。 AutoconfigureIptables = Noの場合、指定された<ONum>番号は、手動で追加する必要があるルータインテグレーションルール番号5で使用する必要があります。</div> <p data-bbox="790 728 1013 757">デフォルト値 : Auto</p>
OutputDivertConnectTransparently {Yes / No}	<p data-bbox="790 786 1444 880">送信接続のために監視されたパケットの送信者(クライアント)のIPアドレスを使用して、受信者(サーバー)に接続するためのエミュレーションモードを有効/無効にします。</p> <p data-bbox="790 913 981 943">使用可能な値 :</p> <ul data-bbox="790 969 1444 1137" style="list-style-type: none">• Yes - 接続を監視するときに、自分のアドレスの代わりに接続をリクエストしたクライアントのアドレスを使用してサーバーに接続します。• No - Dr.Web Firewall for Linuxアドレスからサーバーに接続します。 <p data-bbox="790 1167 1444 1261">クライアントとDr.Web Firewall for Linuxアドレスは通常、送信接続監視モードでは同じであるため、デフォルト値はNoになります。</p> <p data-bbox="790 1288 981 1317">デフォルト値 : No</p>
InputDivertEnable {Yes / No}	<p data-bbox="790 1346 1444 1440">受信接続(つまりローカルホストに接続があるリモートホストのアプリケーションによって開始された接続)の監視を有効/無効にします。</p> <p data-bbox="790 1473 981 1503">使用可能な値 :</p> <ul data-bbox="790 1529 1364 1608" style="list-style-type: none">• Yes - 受信接続の監視と処理を有効にします。• No - 受信接続の監視と処理を無効にします。 <div data-bbox="826 1624 1449 1899" style="background-color: #fff9c4; padding: 10px;"> この設定は、AutoconfigureIptables = Noの場合に、手動で追加または削除されるルータインテグレーションルール番号6を追加または削除します。無効な値を指定した場合、コンポーネントの起動は失敗します。</div> <p data-bbox="790 1921 997 1951">デフォルト値 : No</p>



パラメータ	説明
<p>InputDivertNfqueueNumber {integer / Auto}</p>	<p>Dr.Web Firewall for Linuxが、受信接続を開始するSYNパッケージを取得するキュー番号 <i>NFQUEUE</i></p> <p>使用可能な値：</p> <ul style="list-style-type: none">• <integer> - <i>NFQUEUE</i>で監視された送信接続のSYNパケットを監視するためのキュー番号 <INum>• Auto - Dr.Web Firewall for Linuxは適切なキュー番号を自動的に選択できます(推奨)。 <div data-bbox="828 584 1449 1016" style="border: 1px solid #ccc; background-color: #fff9c4; padding: 10px;"><p> <INum>番号を手動で割り当てるときは、(NetFilterルール経由を含む)接続とパケットを管理する他のアプリケーションが、相応するキュー番号を使用していないことを確認してください。無効な値を指定した場合、コンポーネントの起動は失敗します。</p><p>AutoconfigureIptables = Noの場合、指定された <INum>番号は、手動で追加する必要があるルーティングルール番号6で使用する必要があります。</p></div> <p>デフォルト値 : Auto</p>
<p>InputDivertConnectTransparently {Yes / No}</p>	<p>受信接続のために監視されたパケットの送信者(クライアント)のIPアドレスを使用して、受信者(サーバー)に接続するためのエミュレーションモードを有効/無効にします。</p> <p>使用可能な値：</p> <ul style="list-style-type: none">• Yes - 接続を監視するときに、自分のアドレスの代わりに接続をリクエストしたクライアントのアドレスを使用してサーバーに接続します。• No - Dr.Web Firewall for Linuxアドレスからサーバーに接続します。 <p>受信接続監視モードでは、すべてのトラフィックがDr.Web Firewall for Linuxを通過するため、不正なクライアントのアドレスを使用してサーバーに安全に接続する可能性があります。これがデフォルト値がYesである理由です。</p> <p>デフォルト値 : Yes</p>
<p>ForwardDivertEnable {Yes / No}</p>	<p>トランジット接続(つまりその他のリモートホストに接続があるリモートホストのアプリケーションによって開始された接続)の監視を有効/無効にします。</p> <p>使用可能な値：</p> <ul style="list-style-type: none">• Yes - トランジット接続の監視と処理を有効にします。• No - トランジット接続の監視と処理を無効にします。



パラメータ	説明
	<div data-bbox="826 264 1449 479" style="background-color: #fff9c4; padding: 10px;"> この設定は、 AutoconfigureIptables = Noの 場合に、手動で追加または削除される <u>ルーティングルール</u>番号7を追加または 削除します。</div> <p data-bbox="788 504 976 533">デフォルト値 : No</p>
ForwardDivertNfqueueNumber {integer / Auto}	<p data-bbox="788 562 1444 622">Dr.Web Firewall for Linuxが、トランジット接続を開始する SYNパッケージを取得するキュー番号 <i>NFQUEUE</i></p> <p data-bbox="788 658 976 687">使用可能な値 :</p> <ul data-bbox="788 712 1444 853" style="list-style-type: none">• <integer> - <i>NFQUEUE</i>で監視されたトランジット接続 のSYNパケットを監視するためのキュー番号 <FNum>• Auto - Dr.Web Firewall for Linuxは適切なキュー番号 を自動的に選択できます(推奨)。 <div data-bbox="826 875 1449 1308" style="background-color: #fff9c4; padding: 10px;"> <FNum>番号を手動で割り当てるとき は、(NetFilterルール経由を含む)接続 とパケットを管理する他のアプリケーション が、相応するキュー番号を使用してい ないことを確認してください。無効な値 を指定した場合、コンポーネントの起動 は失敗します。 AutoconfigureIptables = Noの 場合、指定された <FNum>番号は、手 動で追加する必要がある<u>ルーティングル</u> <u>ール</u>番号7で使用してください。</div> <p data-bbox="788 1335 1008 1364">デフォルト値 : Auto</p>
ForwardDivertConnectTransparently {Yes / No}	<p data-bbox="788 1391 1444 1487">トランジット接続のために監視されたパケットの送信者(ク ライアント)のIPアドレスを使用して受信者(サーバー)に 接続するためのエミュレーションモード。</p> <p data-bbox="788 1523 976 1552">使用可能な値 :</p> <ul data-bbox="788 1576 1444 1749" style="list-style-type: none">• Yes - 接続を監視するときに、自分のアドレスの代わり に接続をリクエストしたクライアントのアドレスを使用して サーバーに接続します。• No - Dr.Web Firewall for Linuxアドレスからサーバーに接 続します。 <p data-bbox="788 1774 1444 1995">トランジット接続監視モードでは、すべてのトラフィックが Dr.Web Firewall for Linuxがインストールされているのと同 じホスト(ルーター)を通過するという保証はないため、正 しい動作のデフォルト値はNoになります。保護されたアプリ ケーションが同じルーターを使用することがネットワーク設 定によって保証されている場合、このパラメータをYesに設 定できます。この場合は、Dr.Web Firewall for Linuxがサー</p>



パラメータ	説明
	<p>バーに接続するときは常にクライアントのアドレスへの接続を評価します。</p> <p>デフォルト値 : No</p>
<p>ExcludedProc <i>{path to file}</i></p>	<p>プロセスのホワイトリスト(ネットワークアクティビティが監視されないプロセス)</p> <p>リストをパラメータ値として指定できます。リストの値は、コンマ(引用符内の各値)で区切る必要があります。パラメータはセクションで複数回指定できます(この場合、そのすべての値が1つのリストにまとめられます)。</p> <p>例: プロセスのリストにwgetとcurlを追加します。</p> <ol style="list-style-type: none">設定ファイルに値を追加します。<ul style="list-style-type: none">1行に2つの値:<pre data-bbox="831 808 1442 949">[LinuxFirewall] ExcludedProc = "/usr/bin/wget", "/usr/bin/curl"</pre>2行(1行に1つの値):<pre data-bbox="831 1005 1442 1146">[LinuxFirewall] ExcludedProc = /usr/bin/wget ExcludedProc = /usr/bin/curl</pre>drweb-ctl cfset コマンドを使用して値を追加します。<pre data-bbox="831 1234 1442 1469"># drweb-ctl cfset LinuxFirewall.ExcludedProc - a /usr/bin/wget # drweb-ctl cfset LinuxFirewall.ExcludedProc - a /usr/bin/curl</pre> <div data-bbox="831 1491 1442 1827" style="background-color: #fff9c4; padding: 10px;"><p> このパラメータで示されるプロセスリストの実際の使用方法は、Dr.Web Firewall for Linuxに定義されているスキャンルールでの使用方法によって決まります。</p><p>デフォルトルールのリスト(以下参照)は、リストからの全プロセスのトラフィックがスキャンせずに許可されることを保証します。</p></div> <p>デフォルト値 : (未設定)</p>
<p>UnwrapSsl <i>{Boolean}</i></p>	<p>SSL/TLS接続を介して転送された暗号化トラフィックをスキャンします。</p>



パラメータ	説明
	<div data-bbox="826 264 1449 707" style="background-color: #e6f2e6; padding: 10px;"> 最近の実行例では、この変数の値は保護されたトラフィックの処理に影響しません。処理を管理するには、SET Unwrap_SSL = true/falseアクションを含むルールを作成する必要があります(以下参照)。 drweb-ctlユーティリティのcfsetコマンドまたはWebインターフェースを使用してこのパラメータの値を変更した場合、影響を受ける依存ルールが自動的に適応します。</div> <p data-bbox="788 730 979 763">デフォルト値: No</p>
BlockInfectionSource {Boolean}	<p data-bbox="788 786 1430 853">悪意のあるソフトウェア (<i>InfectionSource</i>カテゴリーに含まれる)を含むWebサイトへの接続試行をブロックします。</p> <p data-bbox="788 882 1430 949">ブロックをアクティブにするには、次のルールを設定に追加する必要があります(以下の詳細を参照)。</p> <div data-bbox="788 969 1441 1106" style="border: 1px solid #ccc; padding: 5px;"><pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre></div> <p data-bbox="788 1122 995 1155">デフォルト値: Yes</p>
BlockNotRecommended {Boolean}	<p data-bbox="788 1176 1449 1243">非推奨サイト (<i>NotRecommended</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p data-bbox="788 1272 1430 1339">ブロックをアクティブにするには、次のルールを設定に追加する必要があります(以下の詳細を参照)。</p> <div data-bbox="788 1359 1441 1496" style="border: 1px solid #ccc; padding: 5px;"><pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre></div> <p data-bbox="788 1512 995 1545">デフォルト値: Yes</p>
BlockAdultContent {Boolean}	<p data-bbox="788 1568 1430 1635">アダルトコンテンツ (<i>AdultContent</i>カテゴリーに含まれる)を含むWebサイトへの接続試行をブロックします。</p> <p data-bbox="788 1664 1430 1731">ブロックをアクティブにするには、次のルールを設定に追加する必要があります(以下の詳細を参照)。</p> <div data-bbox="788 1751 1441 1888" style="border: 1px solid #ccc; padding: 5px;"><pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre></div> <p data-bbox="788 1904 979 1937">デフォルト値: No</p>



パラメータ	説明
BlockViolence {Boolean}	<p>暴力的描写 (<i>Violence</i>カテゴリーに含まれる)を含むWebサイトへの接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockWeapons {Boolean}	<p>武器に関するWebサイト (<i>Weapons</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockGambling {Boolean}	<p>ギャンブルのWebサイト (<i>Gambling</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockDrugs {Boolean}	<p>麻薬に関するWebサイト (<i>Drugs</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockObsceneLanguage {Boolean}	<p>卑猥な表現 (<i>ObsceneLanguage</i>カテゴリーに含まれる)を含むWebサイトへの接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p>



パラメータ	説明
	<pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockChats {Boolean}	<p>チャットWebサイト (<i>Chats</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockTerrorism {Boolean}	<p>テロリズムに関するWebサイト (<i>Terrorism</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockFreeEmail {Boolean}	<p>無料メールサービスのWebサイト (<i>FreeEmail</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockSocialNetworks {Boolean}	<p>ソーシャルネットワーキングWebサイト (<i>SocialNetworks</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>



パラメータ	説明
BlockDueToCopyrightNotice {Boolean}	<p>著作権者のリクエストに従って追加されたWebサイト (<i>DueToCopyrightNotice</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockOnlineGames {Boolean}	<p>オンラインゲームWebサイト (<i>OnlineGames</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockAnonymizers {Boolean}	<p>アノマイザーWebサイト (<i>Anonymizers</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockCryptocurrencyMiningPools {Boolean}	<p>仮想通貨マイニングのための一般的なサービスへのアクセスを提供するWebサイト (<i>CryptocurrencyMiningPool</i>カテゴリーに含まれる)への接続試行をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockJobs {Boolean}	<p>求人検索Webサイト (<i>Jobs</i>カテゴリーに含まれます)への接続試行をブロックします。</p>



パラメータ	説明
	<p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre data-bbox="791 353 1442 488">url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
Whitelist <i>{domain list}</i>	<p>ドメインのホワイトリスト(ブロックされたカテゴリに含まれている場合でも、ユーザーの接続が許可されているドメイン。さらに、このリストに示されているドメインのすべてのサブドメインへユーザーがアクセスすることが許可されます)。</p> <p>リストの値は、コンマ(引用符内の各値)で区切る必要があります。パラメータはセクションで複数回指定できます(この場合、そのすべての値が1つのリストにまとめられます)。</p> <p>例: ドメインexample.comとexample.netのリストに追加します。</p> <ol style="list-style-type: none">設定ファイルに値を追加します。<ul style="list-style-type: none">1つの文字列に2つの値:<pre data-bbox="831 1025 1442 1160">[LinuxFirewall] Whitelist = "example.com", "example.net"</pre>2つの文字列(文字列ごとに1つの値):<pre data-bbox="831 1223 1442 1357">[LinuxFirewall] Whitelist = example.com Whitelist = example.net</pre>drweb-ctl cfset コマンドを使用して値を追加します。<pre data-bbox="831 1451 1442 1682"># drweb-ctl cfset LinuxFirewall.Whitelist -a example.com # drweb-ctl cfset LinuxFirewall.Whitelist -a example.net</pre>

パラメータ	説明
	<div data-bbox="853 297 922 360"></div> <p data-bbox="970 297 1422 421">このパラメータで示されるドメインリストの実際の使用方法は、Dr.Web Firewall for Linuxに定義されているスキャンルールでの使用方法によって決まります。</p> <p data-bbox="970 454 1422 869">デフォルトルールのリスト(下記参照)は、ブロックされるWebソースカテゴリーのリストのドメインがこのリストに含まれている場合でも、このリストのドメイン(およびそのサブドメイン)へのアクセスが提供されることを保証します(ただしHTTPプロトコルを経由したサーバーへのリクエストの場合のみ)。さらに、このデフォルトのルールセットは、ホワइटリストドメインからダウンロードしたデータが脅威に対してスキャンされることを保証します(データはレスポンスで返され、変数directionには値responseがあるため)。</p> <p data-bbox="790 920 1066 949">デフォルト値: (未設定)</p>
Blacklist <i>{domain list}</i>	<p data-bbox="790 976 1449 1133">ブラックリストとして使用できるドメインのリスト(つまり、これらのドメインがブロックされたカテゴリーに含まれていない場合でも、ユーザーの接続が禁止されているドメインのリスト。さらに、このリストに示されているドメインのすべてのサブドメインへユーザーがアクセスすることが禁止されます)。</p> <p data-bbox="790 1167 1449 1261">リストの値は、コンマ(引用符内の各値)で区切る必要があります。パラメータはセクションで複数回指定できます(この場合、そのすべての値が1つのリストにまとめられます)。</p> <p data-bbox="790 1294 1433 1357">例: ドメインexample.comとexample.netのリストに追加します。</p> <p data-bbox="790 1384 1193 1413">1. 設定ファイルに値を追加します。</p> <ul data-bbox="831 1429 1134 1458" style="list-style-type: none">• 1つの文字列に2つの値: <div data-bbox="831 1469 1442 1608"><pre>[LinuxFirewall] Blacklist = "example.com", "example.net"</pre></div> <ul data-bbox="831 1626 1302 1655" style="list-style-type: none">• 2つの文字列(文字列ごとに1つの値): <div data-bbox="831 1666 1442 1805"><pre>[LinuxFirewall] Blacklist = example.com Blacklist = example.net</pre></div>



パラメータ	説明
	<p>2. drweb-ctl cfset コマンドを使用して値を追加します。</p> <pre data-bbox="831 338 1442 568"># drweb-ctl cfset LinuxFirewall.Blacklist -a example.com # drweb-ctl cfset LinuxFirewall.Blacklist -a example.net</pre> <div data-bbox="831 595 1442 1061"><p>このパラメータで示されるドメインリストの実際の使用方法は、Dr.Web Firewall for Linuxに定義されているスキャンルールでの使用方法によって決まります。</p><p>デフォルトルールのリスト (以下参照) は、このリストのドメイン (およびそのサブドメイン) へのアクセスがHTTPプロトコル上で常に禁止されることを保証します。このドメインがホワイトリストとブラックリストに同時に追加される場合、デフォルトのルールにより、そのドメインへのユーザーアクセスは確実にブロックされます。</p></div> <p>デフォルト値: (未設定)</p>
ScanTimeout {time interval}	<p>SpIDer Gateによって開始された1つのファイルに対するスキャンのタイムアウト</p> <p>指定可能な値: 1秒 (1s) から1時間 (1h) まで。</p> <p>デフォルト値: 30s</p>
HeuristicAnalysis {On / Off}	<p>既知の脅威を検出するためのヒューリスティック解析を有効／無効にします。ヒューリスティック解析における検出の信頼性は高いですが、ウイルススキャンにかかる時間が長くなります。</p> <p>ヒューリスティックアナライザによって検出された脅威に適用されるアクションは、BlockSuspiciousパラメータ値として指定します。</p> <p>使用可能な値:</p> <ul data-bbox="791 1693 1410 1805" style="list-style-type: none">● On - スキャン時のヒューリスティック解析を有効にします。● Off - ヒューリスティック解析を無効にします。 <p>デフォルト値: On</p>
PackerMaxLevel {integer}	<p>圧縮されたオブジェクトの最大ネスティングレベル。圧縮されたオブジェクトは、特別なソフトウェア (UPX、PELock、PECompact、Petite、ASPack、Morphineなど) で圧縮され</p>



パラメータ	説明
	<p>た実行コードです。そのようなオブジェクトには、圧縮されたオブジェクトなども含まれている、他の圧縮されたオブジェクトが含まれる場合があります。このパラメータの値はネスティングの上限を指定します。この上限を超えると、他の圧縮されたオブジェクト内の圧縮されたオブジェクトはスキャンされません。</p> <p>ネスティングレベルの制限はありません。値を0に設定すると、ネストされたオブジェクトはスキャンされません。</p> <p>デフォルト値：8</p>
ArchiveMaxLevel <i>{integer}</i>	<p>他のアーカイブが含まれる可能性のあるアーカイブ(zip、rarなど)の最大ネスティングレベル(これらのアーカイブには他のアーカイブなどが含まれる場合もあります)。このパラメータの値はネスティングの上限を指定します。この上限を超えると、他のアーカイブに含まれるアーカイブはスキャンされません。</p> <p>ネスティングレベルの制限はありません。値を0に設定すると、ネストされたオブジェクトはスキャンされません。</p> <p>デフォルト値：8</p>
MailMaxLevel <i>{integer}</i>	<p>他のファイルが含まれる可能性のあるメーラーのファイル(pst、tbbなど)の最大ネスティングレベル(これらのファイルには他のファイルなどが含まれる場合もあります)。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他のオブジェクト内のオブジェクトはスキャンされません。</p> <p>ネスティングレベルの制限はありません。値を0に設定すると、ネストされたオブジェクトはスキャンされません。</p> <p>デフォルト値：8</p>
ContainerMaxLevel <i>{integer}</i>	<p>他のオブジェクトが含まれる他のタイプのオブジェクト(HTMLページ、jarファイルなど)の最大ネスティング。このパラメータの値はネスティングの上限を指定します。この上限を超えると、他のオブジェクト内のオブジェクトはスキャンされません。</p> <p>ネスティングレベルの制限はありません。値を0に設定すると、ネストされたオブジェクトはスキャンされません。</p> <p>デフォルト値：8</p>
MaxCompressionRatio <i>{integer}</i>	<p>圧縮されたオブジェクトの最大圧縮率(非圧縮サイズと圧縮サイズの比率)。オブジェクトの比率が制限を超えると、SpIDer Gateによって開始されたファイルスキャン中にそのオブジェクトはスキップされます。</p> <p>圧縮率には2よりも小さい値は指定できません。</p> <p>デフォルト値：500</p>



パラメータ	説明
BlockKnownVirus {Boolean}	<p>既知の脅威を含むデータの受信または送信をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : Block as _match</pre> <p>デフォルト値: Yes</p>
BlockSuspicious {Boolean}	<p>ヒューリスティックアナライザによって検出された未知の脅威を含むデータの受信または送信をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : Block as _match</pre> <p>デフォルト値: Yes</p>
BlockAdware {Boolean}	<p>アドウェアを含むデータの受信または送信をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : Block as _match</pre> <p>デフォルト値: Yes</p>
BlockDialers {Boolean}	<p>ダイヤラープログラムを含むデータの受信または送信をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : Block as _match</pre> <p>デフォルト値: Yes</p>
BlockJokes {Boolean}	<p>ジョークプログラムを含むデータの受信または送信をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p>



パラメータ	説明
	<pre>threat_category in "LinuxFirewall.BlockThreat" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockRiskware {Boolean}	<p>リスクウェアを含むデータの受信または送信をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockHacktools {Boolean}	<p>ハッキングツールを含むデータの受信または送信をブロックします。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (以下の詳細を参照)。</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockUnchecked {Boolean}	<p>スキャンできないトラフィックをブロックします。</p> <div style="border: 1px solid #ccc; background-color: #e6ffe6; padding: 10px; margin: 10px 0;"><p> このパラメータ値は、エラーのためにtrueまたはfalseに評価することが不可能なルールの処理に影響します。Noを指定した場合、ルールは実行されていないルールとしてスキップされます。Yesを指定した場合、Block as BlackListアクションが実行されます。</p></div> <p>デフォルト値 : No</p>
InterceptHook {path to file / Lua function}	<p>Luaで接続を処理するためのスクリプトまたはそのスクリプトを含むファイルへのパス (Luaでの接続処理セクションを参照)。</p> <p>使用できないファイルを指定すると、コンポーネントを読み込む際にエラーが表示されます。</p> <p>デフォルト値 :</p> <pre>local dwl = require 'drweb.lookup'</pre>



パラメータ	説明
	<pre>function intercept_hook(ctx) -- do not check if group == Root.TrustedGroup if ctx.divert == "output" and ctx.group == "drweb" then return "pass" end -- do not check connections from privileged ports -- except FTP active mode if ctx.src.port >= 0 and ctx.src.port <= 1024 and ctx.src.port ~= 20 then return "pass" end return "check" end</pre>



接続スキャンの設定を変更しても、変更を加える前にアプリケーションによってすでに確立されている接続のスキャンには影響しません。それらをすでに実行中のアプリケーションに適用する必要がある場合は、アプリケーションを再起動するなどして、アプリケーションを強制的に切断してから再度接続する必要があります。

トラフィックモニタリングとアクセスブロックのルール

このセクションには、上記のパラメータの他、11個のルールセットRuleSet*(RuleSet0、...、RuleSet10)も含まれます。これらは、トラフィックスキャン、Webリソースへのユーザーアクセスのブロック、インターネットからのコンテンツのダウンロードのブロックを直接管理します。条件の一部の値(IPアドレス範囲、Webサイトカテゴリーのリスト、Webソースのホワイト/ブラックリストなど)については、テキストファイルから読み込まれる値の置き換えがあり、LDAPを介して外部データソースから抽出されます(Dr.Web LookupDコンポーネントが使用されます)。接続を設定する際には、最終的な解決を含むルールが見つかるまで、すべてのルールが昇順で検査されます。ルールリストのギャップは無視されます。

ルールについては、付録Dの[トラフィックモニタリングのルール](#)のセクションで詳しく説明されています。

ルールを表示して編集する

ルールリストを簡単に編集するために未設定のものが残されています。つまり、ルールが指定されていないRuleSet <i>があります (<i> - RuleSetルールセット番号)。RuleSet <i>以外の項目を追加することはできませんが、RuleSet <i>の要素内のルールは追加および削除できます。ルールの表示と編集は、次のいずれかの方法で実行できます。

- (任意のテキストエディターで) **設定ファイル**設定ファイルを表示して編集する(このファイルにはデフォルトとは異なる値のパラメータのみが保存されます)。



- [Web管理インターフェース](#)を使用する(インストールされている場合)。
- コマンドラインベースのインターフェース[Dr.Web Ctl](#)(`drweb-ctl cfshow`および`drweb-ctl cfset`[コマンド](#))を使用する。



ルールを編集して設定ファイルを変更した場合は、その変更を適用するためにDr.Web for UNIX Internet Gatewaysを再起動します。それには`drweb-ctl reload`コマンドを使用します。

ルールを表示するには、`drweb-ctl cfshow`コマンドを使用します。

ルールセット`LinuxFirewall.RuleSet1`のコンテンツを表示するには、次のコマンドを使用します。

```
# drweb-ctl cfshow LinuxFirewall.RuleSet1
```

ルールを編集するには、`drweb-ctl cfset`コマンドを使用します(以降、`<rule>`はルールのテキストです)。

- `LinuxFirewall.RuleSet1`セットのすべてのルールを新しいルールで置き換えます。

```
# drweb-ctl cfset LinuxFirewall.RuleSet1 '<rule>'
```

- `LinuxFirewall.RuleSet1`ルールセットに新しいルールを次のように追加します。

```
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 '<rule>'
```

- `LinuxFirewall.RuleSet1`セットから特定のルールを次のように削除します。

```
# drweb-ctl cfset -e LinuxFirewall.RuleSet1 '<rule>'
```

- `LinuxFirewall.RuleSet1`ルールセットを次のようにデフォルトの状態にリセットします。

```
# drweb-ctl cfset -r LinuxFirewall.RuleSet1
```

`drweb-ctl`ツールを使用してルールのリストを編集するときは、追加するルールのテキストを一重引用符または二重引用符で囲み、ルール自体のテキストに二重引用符が含まれている場合には、ルールのテキスト内にある二重引用符の前にバックスラッシュ(「\」)をエスケープ文字として使用します。

設定の`RuleSet` `<i>`変数には、ルールの格納について次のような特徴があります。

- 無条件ルールを追加するときは、条件部分とコロンを省略できます。ただし、そのようなルールは常にルールのリストに文字列「 : `<action>`」として格納されます。
- 複数のアクションを含むルール(「 `<condition>` : `<action 1>`, `<action 2>`」など)を追加すると、そのようなルールは基本ルールのチェーン「 `<condition>` : `<action 1>`」と「 `<condition>` : `<action 2>`」に変更されます。
- ロギングまたはルールは、条件部分で条件の離接(論理和)を許可しないため、論理和を実装するには、各ルールに離接語条件がある条件で一連のルールを記録する必要があります。



接続をスキップするための無条件ルール(Passアクション)をLinuxFirewall.RuleSet1セットに追加するには、次のコマンドのみを実行します。

```
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 'Pass'
```

ただし、指定したルールセットからこのルールを削除するには、次のコマンドを実行する必要があります。

```
# drweb-ctl cfset -e LinuxFirewall.RuleSet1 ' : Pass'
```

LinuxFirewall.RuleSet1ルールを、接続用の標準テンプレートへのパスを未解決アドレスから変更してブロックを実行するルールセットに追加するには、次のコマンドを実行する必要があります。

```
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 'src_ip not in  
file("/etc/trusted_ip") : set http_template_dir = "mytemplates", Block'
```

ただし、このコマンドでは指定したセットに2つのルールが追加されるため、ルールのセットからこれらのルールを削除するには、次の2つのコマンドを実行する必要があります。

```
# drweb-ctl cfset -e LinuxFirewall.RuleSet1 'src_ip not in  
file("/etc/trusted_ip") : set http_template_dir = "mytemplates"  
# drweb-ctl cfset -e LinuxFirewall.RuleSet1 'src_ip not in  
file("/etc/trusted_ip") : Block'
```

「悪意のあるオブジェクト*KnownVirus*や*Terrorism*カテゴリーに該当するURLが検出された場合はブロックする」などのルールをLinuxFirewall.RuleSet1ルールセットに追加するには、このルールセットに次の2つのルールを追加する必要があります。

```
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 'threat_category in (KnownVirus)  
: Block as _match'  
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 'url_category in (Terrorism) :  
Block as _match'
```

ルールのセットからこれらのルールを削除する場合にも、2つのコマンドを実行する必要があります(上記の例を参照)。

デフォルトのルールセット

デフォルトでは、次のブロックルールセットが指定されています。

```
RuleSet0 =  
RuleSet1 = divert output : set HttpTemplatesDir = "output"  
RuleSet1 = divert output : set MailTemplatesDir = "firewall"  
RuleSet1 = divert input : set HttpTemplatesDir = "input"  
RuleSet1 = divert input : set MailTemplatesDir = "server"  
RuleSet1 = proc in "LinuxFirewall.ExcludedProc" : Pass  
RuleSet1 = : set Unwrap_SSL = false  
RuleSet2 =  
RuleSet3 =  
RuleSet4 =  
RuleSet5 = protocol in (Http), direction request, url_host in
```



```
"LinuxFirewall.Blacklist" : Block as BlackList
RuleSet5 = protocol in (Http), direction request, url_host in
"LinuxFirewall.Whitelist" : Pass
RuleSet6 =
RuleSet7 = protocol in (Http), direction request, url_category in
"LinuxFirewall.BlockCategory" : Block as _match
RuleSet8 =
RuleSet9 = protocol in (Http), divert input, direction request,
threat_category in "LinuxFirewall.BlockThreat" : Block as _match
RuleSet9 = protocol in (Http), direction response, threat_category in
"LinuxFirewall.BlockThreat" : Block as _match
RuleSet9 = protocol in (Sntp), threat_category in
"LinuxFirewall.BlockThreat" : REJECT
RuleSet9 = protocol in (Sntp), url_category in "LinuxFirewall.BlockCategory"
: REJECT
RuleSet9 = protocol in (Sntp), total_spam_score gt 0.80 : REJECT
RuleSet9 = protocol in (Pop3, Imap), threat_category in
"LinuxFirewall.BlockThreat" : REPACK as _match
RuleSet9 = protocol in (Pop3, Imap), url_category in
"LinuxFirewall.BlockCategory" : REPACK as _match
RuleSet9 = protocol in (Pop3, Imap), total_spam_score gt 0.80 : REPACK as
_match
RuleSet10 =
```

最初のルールは、`ExcludedProc`パラメータ(上記を参照)で指定されたプロセスによって接続が確立された場合、他の条件を検査せずに接続をスキップすることを示します。次のルール(条件なしで実行されます)は保護された接続のラップ解除をブロックします。このルールとその下位にあるすべてのルールは、接続が除外されたプロセスで設定されていない場合にのみ考慮されます。また、後続のすべてのルールはプロトコルに依存するため、保護された接続のラップ解除が無効になっている場合は、条件がtrueと評価されるかどうかを定義できないため、ルールは実行されません。

次のルールは、送信HTTP接続に対する処理を制御します。

1. 接続が確立されたホストがブラックリストに含まれている場合、そのホストがブラックリストに含まれているため、接続はブロックされます。他のスキャンは実行されません。
2. ホストがホワイトリストに含まれている場合、接続はスキップされ、他のスキャンは実行されません。
3. クライアントからリクエストされたURLが、望ましくないWebリソースのカテゴリに含まれている場合は、脅威が検出されたために接続がブロックされます。他のスキャンは実行されません。
4. HTTP経由の脅威があるリモートホストから受信したレスポンスに、ブロックされたカテゴリに属する脅威が含まれる場合、その脅威が検出されたために接続がブロックされます。他のスキャンは実行されません。
5. ローカルホストからリモートホストに移行したデータに、ブロックされたカテゴリに属する脅威が含まれる場合、その脅威が検出されたために接続がブロックされます。他のスキャンは実行されません。

この5つのルールは、`InspectHttp`パラメータでOnが指定されている場合にのみ機能します。それ以外の場合、これらのルールはどれも機能しません。

RuleSet9で指定される次の6つのルールは、メールプロトコル(SMTP、POP3、IMAPプロトコル)を介して送受信されるデータのスキャンを制御します。これらのルールは、次の場合に有効になります。

- 送信されたメールメッセージに、添付ファイルが含まれている場合
- 送信されたメールメッセージに、望ましくないカテゴリに属するURLが含まれている場合
- 送信されたメールメッセージがスパムとして分類された場合(スパムインデックスが0.8以上)



メールメッセージがSMTPプロトコルを介して送信される場合、メールの伝送(つまり送信または受信)はブロックされますが、IMAPとPOP3プロトコルの場合は、メールはそのコンテンツから悪意のあるコンテンツを削除するために処理(「再パッケージ」)されます。



メールメッセージのスパムの兆候をスキャンするためのコンポーネントであるDr.Web Anti-Spamが使用できない場合、スパムの兆候をスキャンするためのメールメッセージのスキャンは実行されません。この場合、スパムレベルのスキャン(`total_spam_score`値)を含むルールは使用できません。

メール処理ルールは、相応する`Inspect <EmailProtocol>`パラメータに`On`が指定されている場合にのみ実行されることに注意してください。それ以外の場合、これらのルールはどれも実行されません。さらに、送信されたメールメッセージのマルウェアの添付ファイルとスパムの兆候を調べるために、メールスキャン用のDr.Web MailDコンポーネントをインストールする必要があります。このコンポーネントがインストールされていない場合、「検査できません」というエラーのため、送信されたメールはブロックされます。検査できないメッセージの送信を許可するには、`BlockUnchecked = No`パラメータを設定します(上記を参照)。また、メールスキャンコンポーネントがインストールされていない場合は、`InspectSmtp`、`InspectPop3`、`InspectImap`パラメータに`No`を指定することをお勧めします。



Dr.Web MailDはDr.Web for UNIX Internet Gatewaysに含まれていません。

トラフィックモニタリングとアクセスブロックのルールの例

1. IPアドレス範囲が`10.10.0.0~10.10.0.254`のユーザーに`Chats`以外のすべてのカテゴリーのWebサイトへのHTTPアクセスを許可する。

```
protocol in (HTTP), src_ip in (10.10.0.0/24), url_category not in (Chats)
: Pass
```

ルール

```
protocol in (HTTP), url_host in "LinuxFirewall.Blacklist" : Block as
BlackList
```

が、指定されたルールより上のルールリストに割り当てられている場合、IPアドレス範囲が`10.10.0.0~10.10.0.254`のユーザーは、ブラックリストのドメイン、つまりパラメータ`LinuxFirewall.Blacklist`にリストされているドメインへのアクセスもブロックされます。また、このルールが下に割り当てられている場合、IPアドレス範囲が`10.10.0.0~10.10.0.254`のユーザーは、ブラックリストのWebサイトにもアクセスできます。

アクション`Pass`は最終的なものであるため、これ以上のルールはチェックされず、したがってダウンロードされたデータのウイルススキャンも実行されません。IPアドレス範囲が`10.10.0.0~10.10.0.254`のユーザーに、ブラックリストに含まれていない`Chats`以外のすべてのカテゴリーのWebサイトへのアクセスを許可し、同時に脅威のダウンロードをブロックするには、次のルールを使用します。

```
protocol in (HTTP), url_category not in (Chats), url_host not in
"LinuxFirewall.Blacklist", threat_category not in
"LinuxFirewall.BlockCategory" : Pass
```



- インターネットからダウンロードしたビデオファイルのコンテンツ(つまり、MIMEタイプが「video/*」のデータ(*はMIMEクラスvideoの任意のタイプ))のスキャンは実行しない。

```
direction response, content_type in ("video/*") : Pass
```

ローカルコンピューターから読み込んだファイル(MIMEタイプが「video/*」のファイルを含む)は、レスポンスではなくリクエストで送信されるために(つまり変数directionには値requestがあるため)スキャンされません。

Luaでの接続処理

このセクションの内容:

- [概要](#)
- [接続処理のスクリプトにおける要件](#)
- [例](#)
- [使用中のテーブル](#)
- [利用可能な補助モジュール](#)

概要

Dr.Web Firewall for LinuxはLuaのプログラムインタプリタを介して対話をサポートします(バージョン5.3.4が使用され、Dr.Web for UNIX Internet Gatewaysと一緒に提供されます)。Luaで書かれたスクリプトは、解析のためにSpIDer Gateに送信される前に、事前接続スキャンのためにコンポーネントによって使用されます。

このスクリプトへのパスがDr.Web Firewall for Linux設定(InterceptHookパラメータ)で指定されている場合、接続はLuaスクリプトで解析されます。それ以外の場合は、コンポーネント設定で指定されているデフォルト設定と処理ルール(RuleSet*パラメータ)を使用して接続処理が実行されます。



接続処理用のLuaスクリプトのその他の例については、次のリンクからご確認ください。
<https://github.com/DoctorWebLtd/drweb-lua-examples/tree/master/firewall>

接続処理のスクリプトにおける要件

このスクリプトには、接続スキャンモジュールのエントリーポイントであるグローバル関数が含まれている必要があります(Dr.Web Firewall for Linuxは、新しく受信した接続を処理するためにこの関数を呼び出します)。この関数は、次の呼び出し規則を満たす必要があります。

- **関数名** - intercept_hook
- **引数** - Lua [コンテキスト](#) テーブルのみ(処理された接続の関数からの情報へのアクセスを提供します。以下の表の説明を参照。)
- **戻り値** - 以下の表のいずれかの文字列値のみ

値	判定の説明
pass	SpIDer Gateによる接続のチェックを行わず、スキップします。



値	判定の説明
check	SpIDer Gateを使用して接続をチェックします。
reject	接続を破棄します（接続を開始したクライアントは、RSTフラグ付きのTCPパッケージを受信します）。
drop	切断します（接続を開始したクライアントは確認応答を受信しません）。

例

1. 次のスクリプトは、Dr.Web Firewall for Linuxによって接続がチェックされないように、すべての接続に対して常にpass判定（スキップ）を返します。

```
-- Function of connection scanning written by the user
function intercept_hook(ctx)
    return "pass" -- do not scan the connection
end
```

2. 次のスクリプトを使用すると、以下の例外を除いて、Dr.Web Firewall for Linuxは確立されているすべての接続をチェックします。

- drwebグループのユーザー権限で実行されているアプリケーションからの送信ローカル接続
- （接続の所有者とその方向に関係なく）権限のあるポートから開始された接続
- ローカルネットワークからのIPアドレスから始まる接続

```
function intercept_hook(ctx)
    -- Do not scan connections, initiated from the local
    -- host (divert == "output") by application under the name of
    -- "drweb" (group == "[drweb]")
    if ctx.divert == "output" and ctx.group == "drweb" then
        return "pass"
    end

    -- Do not scan connections, initiated from
    -- privileged ports (range is from 0 to 1024)
    if ctx.src.port >= 0 and ctx.src.port <= 1024 then
        return "pass"
    end

    -- Do not scan connections from local network IP addresses
    -- (IP address range 127.0.0.1/8)
    if ctx.src.ip.belongs("127.0.0.0/8") then
        return "pass"
    end

    -- Connection is scanned by default
    return "check"
end
```




スクリプトで使用されるテーブル

1. InterceptContextテーブル

このテーブルは、処理された接続に関するデータを`intercept_hook`関数に転送するために使用されます。このデータに基づいて、次のいずれかのアクションを接続に対して実行できます。

- チェックせずにスキップする。
- 接続を中断する。
- チェックのためにSpIDer Gateに接続を送信する。

Dr.Web Firewall for Linuxではテーブルにデータを入力します。テーブルのデータの中には、`intercept_hook`関数が実行されるまでに使用できるものもあります。他のデータ(いわゆる「遅延」データ)は、テーブルの該当するフィールドのリクエストに応じて直接計算されます。

フィールド	説明	データタイプ
<code>src</code>	接続を開始したクライアントのアドレスとポート 例： <pre>if ctx.src.port >= 0 and ctx.src.port <= 1024 then return "pass" end</pre>	TcpEndpoint テーブル
<code>dst</code>	クライアントによって接続が開始されたサーバーのアドレスとポート 例： <pre>if ctx.dst.ip.belongs("10.20.30.41/8") then return "reject" end</pre>	TcpEndpoint テーブル
<code>divert</code>	監視される接続のタイプ： <ul style="list-style-type: none">• "output" - 送信接続• "input" - 受信接続• "forward" - トランジット接続 例： <pre>if ctx.divert == "forward" then return "check" end</pre>	文字列
<code>iface_in</code>	接続が開始されたインターフェースの名前 インターフェース名が特定されていない場合は、 <code>nil</code> 値になります。	文字列
<code>iface_out</code>	接続が開始された後にパケットが送信されたインターフェースの名前 インターフェース名が特定されていない場合は、 <code>nil</code> 値になります。	文字列



フィールド	説明	データタイプ
uid	発信接続を開始したユーザーのID 接続タイプ(divert)が"output"ではない場合、またはUIDを特定できない場合は、nil値になります。	番号
gid	その権限により発信接続が開始されたグループのID 接続タイプ(divert)が"output"ではない場合、またはGIDを特定できない場合は、nil値になります。	番号
user	発信接続を開始したユーザーの名前 接続タイプ(divert)が"output"ではない場合、またはUIDを特定できない場合は、nil値になります。	文字列
group	その権限により発信接続が開始されたグループの名前 接続タイプ(divert)が"output"ではない場合、またはUIDを特定できない場合は、nil値になります。	文字列
pid	発信接続を開始したプロセスのID 接続タイプ(divert)が"output"ではない場合、またはPIDを特定できない場合は、nil値になります。	番号
exe_path	送信接続を開始したアプリケーションファイルへの実行パス 接続タイプ(divert)が"output"ではない場合、または実行パスを特定できない場合は、nil値になります。	文字列
無効になったメタメソッド: なし		

2. TcpEndpointテーブル

このテーブルでは接続ポイント(クライアントまたはサーバー)のアドレスを指定します。

フィールド	説明	データタイプ
ip	IPアドレス	IpAddress テーブル
port	ポート番号	番号
無効になったメタメソッド:		
<ul style="list-style-type: none"> __tostring - TcpEndpointを文字列に変換する関数。例: "127.0.0.1:443"(IPv4)または "[::1]:80"(IPv6) __concat - TcpEndpointを文字列に連結する関数 		

利用可能な補助モジュール

LuaのプログラムスペースでDr.Web for UNIX Internet Gatewaysとやり取りするために、次の特定のモジュールをインポートできます。



モジュール名	機能
drweb	Luaプログラムを起動したDr.Web for UNIX Internet GatewaysコンポーネントのログにLuaプログラムからのメッセージを記録する機能と、Luaプロシージャの非同期実行の手段を提供するモジュール
drweb.lookup	Dr.Web LookupDモジュールを呼び出して外部ソースからデータを要求するためのツールを提供するモジュール

drwebモジュールの内容

1. 機能

このモジュールには、次のような機能があります。

- LuaプログラムからのメッセージをDr.Web for UNIX Internet Gatewaysコンポーネントログに保存する:
 - `log(<level>, <message>)`は<message>文字列をDr.Web for UNIX Internet Gatewaysログに<level>レベル(必要なレベルは、「debug」、「info」、「notice」、「warning」、「error」を使用して定義します)で書き込みます。
 - `debug(<message>)`は<message>文字列をDr.Web for UNIX Internet Gatewaysログに *DEBUG*レベルで書き込みます。
 - `info(<message>)`は<message>文字列をDr.Web for UNIX Internet Gatewaysログに *INFO*レベルで書き込みます。
 - `notice(<message>)`は<message>文字列をDr.Web for UNIX Internet Gatewaysログに *NOTICE*レベルで書き込みます。
 - `warning(<message>)`は<message>文字列をDr.Web for UNIX Internet Gatewaysログに *WARNING*レベルで書き込みます。
 - `error(<message>)`は<message>文字列をDr.Web for UNIX Internet Gatewaysログに *ERROR*レベルで書き込みます。
- Luaプロシージャの同期を管理する:
 - `sleep(<sec.>)`はこのLuaプロシージャインスタンスの実行を指定された秒数で一時停止します。
 - `async(<Lua function>[, <argument list>])`は、指定された関数を非同期的に起動し、指定された引数リストに渡します。`async`関数呼び出しはすぐに完了し、戻り値(Futureテーブル)を使用すると、<Lua function>の結果を取得できます。
- [IpAddress](#)テーブルにIPアドレスを追加する:
 - `ip(<address>)`は、IpAddressテーブルの形式で<address>文字列として送信される、IPアドレスを指定します。IPv4またはIPv6アドレスのいずれかを使用できます。
- テキストファイルから外部データをアップロードする:
 - `load_set(<file path>)`は、指定されたテキストファイルのコンテンツからtrue値を含むテーブルを生成します。ファイルから読み取られた文字列はキーとして使用されます。空の文字列と空白を含む文字列は無視されます。
 - `load_array(<file path>)`は、指定されたテキストファイルのコンテンツから文字列の配列を生成します。空の文字列と空白文字のみで構成される文字列は無視され、配列には含まれません。



2. テーブル

- Futureテーブルは、`async`関数を使用して関数を実行した後の保留中の結果を表します。

フィールド	説明	データタイプ
<code>wait</code>	<code>async</code> 関数を使用して開始した関数の結果を返す関数。関数がまだ実行を完了していない場合は、完了を待って結果を返します。 <code>wait</code> が呼び出される前に関数が完了した場合、結果はすぐに返されます。開始された関数が失敗した場合、 <code>wait</code> 呼び出しは同じエラーを生成します。	機能
無効になったメタメソッド: なし		

- `IpAddress`テーブルはIPアドレスを表します。

フィールド	説明	データタイプ
<code>belongs</code>	<p><code>IpAddress</code>テーブルに保存されているIPアドレスが、指定されたサブネット (IPアドレス範囲) に所属しているかどうかを確認する関数</p> <p>"<IP address>"または "<IP address>/<mask>"のような文字列を唯一の引数として受け取ります。ここで、<IP address>はホストアドレスまたはネットワークアドレス ("127.0.0.1"など)、<mask>はサブネットワークマスク ("255.0.0.0"などのIPアドレスとして、または "8"などの数値形式で指定できます) です。</p> <p>次のブール値を返します。</p> <ul style="list-style-type: none">• <code>true</code>は、アドレスが指定されたアドレスの少なくとも1つと等しいか、指定されたサブネット (IPアドレスの範囲) の少なくとも1つに属していることを示します。• <code>false</code> - それ以外の場合。	機能
無効になったメタメソッド:		
<ul style="list-style-type: none">• <code>__tostring</code>は、文字列内の<code>IpAddress</code>を変更する関数 (例: "127.0.0.1" (IPv4) または ":::1" (IPv6)) です。• <code>__concat</code>は、<code>IpAddress</code>を文字列に結合する関数です。• <code>__eq</code>は、2つの<code>IpAddress</code>が等しいことを確認する関数です。• <code>__band</code>は、マスクを適用するための関数 (例: <code>dw.ip('192.168.1.2') & dw.ip('255.255.254.0')</code>) です。		

3. 例

- 非同期的に開始される手順によって生成されるメッセージをログへ書き込む:



```
local dw = require "drweb"

-- This function waits two seconds and returns a string,
-- received as an argument
function out_msg(message)
  dw.sleep(2)
  return message
end

-- "Main" function
function intercept(ctx)
  -- Output of a string at the NOTICE level to the Dr.Web for UNIX Internet
  Gateways log
  dw.notice("Intercept function started.")

  -- An asynchronous start of two copies of the out_msg function
  local f1 = dw.async(out_msg, "Hello,")
  local f2 = dw.async(out_msg, " world!")

  -- Waiting for the completion of the copies of the function
  -- out_msg and output its results to log
  -- the Dr.Web for UNIX Internet Gateways log at the DEBUG level
  dw.log("debug", f1.wait() .. f2.wait())
end
```

- スケジュールされた手順を作成する:

```
local dw = require "drweb"

-- Save the table Future in the future global variable in order
-- to preven the removal by the garbage collector
future = dw.async(function()
  while true do
    -- Everyday, the following message is displayed in the log
    dw.sleep(60 * 60 * 24)
    dw.notice("A brand new day began")
  end
end)
```

- 文字列で表現されたIPアドレスを[IpAddress](#)テーブルに変更する:

```
local dw = require "drweb"

local ipv4 = dw.ip("127.0.0.1")
local ipv6 = dw.ip(":::1")
local mapped = dw.ip("::ffff:127.0.0.1")
```

drweb.lookupモジュールの内容

1. 機能

このモジュールは次の機能を提供します。

- `lookup(<request>, <parameters>)`は、Dr.Web LookupDモジュールを介して利用できる外部スト



ページからデータを要求します。<request>引数は、Dr.Web LookupD設定内のセクション(文字列 <type>@<tag>)に対応している必要があります。<parameters>引数は任意で、リクエストを生成するために使用される置換を表します。以下の自動的に許可されるマーカーを使用できます。

- \$u、\$Uは、クライアントコンポーネントによって送信されたユーザー名(user)に自動的に置き換えられます。
- \$d、\$Dは、クライアントコンポーネントによって送信されたドメイン(domain)に自動的に置き換えられます。

これらの引数はテーブルとして設定されます。このテーブルのキーと値は文字列でなければなりません。この関数は、リクエストの結果である文字列の配列を返します。

- check(<checked string>、<request>、<parameters>)は、Dr.Web LookupDモジュールを介して利用できる外部リポジトリで<checked string>が見つかった場合にtrueを返します。引数<request>および<parameters>はlookup関数の引数と同じです(上記を参照)。<checked string>引数は、文字列または__tostringメタメソッドを持つテーブル(つまり、文字列にフォーマットできる)であると想定されます。

2. 例

- LookupD.LDAP.usersデータソースから取得したユーザーのログリストへ書き込む:

```
local dw = require "drweb"
local dwl = require "drweb.lookup"

-- "Main" function
function intercept(ctx)
  -- Writing the string at the NOTICE level to the Dr.Web for UNIX Internet Gateways log
  dw.notice("Intercept function started.")

  -- Writing the request results to the Dr.Web for UNIX Internet Gateways log
  log
  -- to the 'ldap@users' data source
  for _, s in ipairs(dwl.lookup("ldap@users", {user="username"})) do
    dw.notice("Result for request to 'ldap@users': " .. s)
  end
end

end
```



Dr.Web ClamD

Dr.Web ClamDコンポーネントは、Sourcefire, Inc.のアンチウイルス製品Clam AntVirus (ClamAV ®)のコアコンポーネントであるclamdアンチウイルスデーモンのインターフェースを使用してエミュレーションを実行します。このインターフェースにより、ClamAV ®とやり取りできる外部アプリケーションは、アンチウイルススキャンにDr.Web for UNIX Internet Gatewaysを使用できます。

動作原理

このコンポーネントは、ローカルファイルシステムのファイルの内容と、ソケットを介して外部アプリケーションによって送信されたデータのストリームの両方をチェックします。このようなチェックは、外部アプリケーションのリクエストに応じてコンポーネントによって実行されます。さらに、コンポーネントは外部アプリケーションがソケットを介してオープンファイル記述子(ディスクリプタ)を渡したファイルの内容をチェックできます。



渡されたファイル記述子に基づくファイルスキャンは、記述子がローカルのUNIXソケットを介して渡された場合にのみ実行できます。

外部アプリケーションからローカルファイルシステム内のファイルへのパスが提供された場合、コンポーネントはスキャンタスクを[Dr.Web File Checker](#)ファイルチェッカーコンポーネントに送信します。それ以外の場合、コンポーネントは、ソケット経由で受信したデータを[Dr.Web Network Checker](#)に送信します。

デフォルトでは、コンポーネントはDr.Web for UNIX Internet Gatewaysの起動時に自動的に起動されません。コンポーネントの起動を有効にするには、開始パラメータにYesの値を設定し、クライアントアプリケーション用に少なくとも1つの接続ポイントを定義する必要があります。その後、コンポーネントは外部アプリケーションからのファイルまたはデータストリームのスキャンリクエストの待機を開始します。コンポーネントの設定では、外部アプリケーション用に複数の接続ポイントを設定し、必要に応じて各ポイントに異なるスキャン設定を調整できます。

外部アプリケーションは、clamdとの統合モジュールを装備している場合には、HTTPプロキシサーバー(SquidやHAVPなど)として表すことができます。詳細は、[外部アプリケーションとの統合](#)のセクションを参照してください。



検出された脅威をDr.Web for UNIX Internet Gatewaysで駆除することはできません。外部アプリケーションにはスキャンの結果のみが通知されます。そのため、検出された脅威はすべて外部アプリケーションで駆除する必要があります。

コマンドライン引数

Dr.Web ClamDを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-clamd [<parameters>]
```

Dr.Web ClamDは次のパラメータを処理できます。

パラメータ	説明
-------	----



<code>--help</code>	機能: コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了します。 短縮形: <code>-h</code> 引数: なし
<code>--version</code>	機能: このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了します。 短縮形: <code>-v</code> 引数: なし

例:

```
$ /opt/drweb.com/bin/drweb-clamd --help
```

このコマンドは、Dr.Web ClamDに関する簡単なヘルプ情報を出力します。

スタートアップノート

このコンポーネントは、自律モードで(他のコンポーネントから自律的に)OSのコマンドラインから直接起動することはできません。必要に応じて[Dr.Web ConfigD](#)設定デーモンによって自動的に起動されます(原則として、OSの起動時)。コンポーネントの動作を管理するには、Dr.Web for UNIX Internet Gateways用のコマンドラインベース管理ツール[Dr.Web Ctl](#)を使用できます(これは[drweb-ctl](#)コマンドを使用して呼び出されます)。



コマンドラインから製品のこのコンポーネントに関するドキュメントを取得するには、`man 1 drweb-clamd`コマンドを使用します。

設定パラメータ

このセクションの内容

- [コンポーネントパラメータ](#)
- [コンポーネント構成の特別な側面](#)

このコンポーネントは、Dr.Web for UNIX Internet Gatewaysの統合された[設定ファイル](#)の[ClamD]セクションで指定されている設定パラメータを使用します。

コンポーネントパラメータ

セクションには以下のパラメータが含まれています。

パラメータ	説明
<code>LogLevel</code> <i>{logging level}</i>	コンポーネントの ロギングレベル 。 パラメータの値が指定されていない場合は、[Root]セクションのDefaultLogLevelパラメータの値が使用されます。



パラメータ	説明
	デフォルト値: Notice
Log {log type}	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath {path to file}	コンポーネントの実行パス。 デフォルト値: <opt_dir>/bin/drweb-clamd <ul style="list-style-type: none">GNU/Linuxの場合 合: /opt/drweb.com/bin/drweb-clamdFreeBSDの場合 合: /usr/local/libexec/drweb.com/bin/drweb-clamd
Start {Boolean}	このコンポーネントは Dr.Web ConfigD 設定デーモンによって起動される必要があります。 このパラメータにYes値を指定すると、設定デーモンはただちにコンポーネントを開始するように指示されます。また、No値を指定すると、設定デーモンはただちにコンポーネントを終了するように指示されます。 デフォルト値: No
Endpoint.<tag>.ClamdSocket {IP address / UNIX socket}	<tag>という名前の新しい接続ポイントを作成し、ファイルの脅威をスキャンする必要があるクライアントにソケット (IPv4アドレスまたはUNIXソケットのアドレス) を割り当てます。 1つの<tag>ポイントに指定できるソケットは1つのみです。 デフォルト値: 未設定
[Endpoint.<tag>.]DetectSuspicious {Boolean}	ヒューリスティックアナライザによって検出された疑わしいファイルについて通知します。 Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されます。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。 デフォルト値: Yes
[Endpoint.<tag>.]DetectAdware {Boolean}	アドウェアを含むファイルについて通知します。 Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されます。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。 デフォルト値: Yes



パラメータ	説明
[Endpoint.<tag>.]DetectDialers {Boolean}	ダイヤラーを含むファイルについて通知します。 Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されます。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。 デフォルト値: Yes
[Endpoint.<tag>.]DetectJokes {Boolean}	ジョークプログラムを含むファイルについて通知します。 Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されます。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。 デフォルト値: No
[Endpoint.<tag>.]DetectRiskware {Boolean}	リスクウェアを含むファイルについて通知します。 Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されます。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。 デフォルト値: No
[Endpoint.<tag>.]DetectHacktools {Boolean}	ハッキングツールを含むファイルについて通知します。 Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されます。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。 デフォルト値: No
[Endpoint.<tag>.]ReadTimeout {time interval}	クライアントからのデータを待つ最大タイムアウト Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されます。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。 デフォルト値: 5s
[Endpoint.<tag>.]StreamMaxLength {size}	クライアントから受信できるデータの最大サイズ(スキャンするデータをバイトのストリームとして送信するため) Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されます。それ以外の場合は、このパラメータに別の



パラメータ	説明
	<p>値が指定されていないすべてのポイントに設定されます。</p> <p>デフォルト値 : 25mb</p>
[Endpoint.<tag>.]ScanTimeout {time interval}	<p>クライアントから受信した1つのファイル(またはデータの一部)をスキャンする最大時間</p> <p>Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されます。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。</p> <p>指定可能な値 : 1秒(1s)から1時間(1h)まで。</p> <p>デフォルト値 : 3m</p>
[Endpoint.<tag>.]HeuristicAnalysis {On / Off}	<p>スキャンのヒューリスティック解析を有効にします。</p> <p>Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されます。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。</p> <p>デフォルト値 : On</p>
[Endpoint.<tag>.]PackerMaxLevel {integer}	<p>圧縮されたオブジェクトのネスティングレベルの上限。圧縮されたオブジェクトは、特別なソフトウェア(UPX、PELock、PECompact、Petite、ASPack、Morphineなど)で圧縮された実行コードです。そのようなオブジェクトには、圧縮されたオブジェクトなどが含まれる他の圧縮されたオブジェクトが含まれる場合があります。最大ネスティングレベルを超えると、他の圧縮されたオブジェクト内の圧縮されたオブジェクトはスキャンされません。</p> <p>Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されます。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。</p> <p>このパラメータの値は、0より大きい任意の整数に設定できます。値を0に設定すると、ネストされたオブジェクトはスキャンされません。</p> <p>デフォルト値 : 8</p>
[Endpoint.<tag>.]ArchiveMaxLevel {integer}	<p>スキャンできるアーカイブ(zip、rarなど)の最大ネスティングレベル。アーカイブには、他のアーカイブなどを含むアーカイブが含まれる場合があります。最大ネスティングレベルを超えると、アーカイブ内のアーカイブはスキャンされません。</p>



パラメータ	説明
	<p>Endpoint. <tag>のプレフィックスが指定されている場合は、パラメータの値が <tag>接続ポイントにのみ設定されます。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。</p> <p>このパラメータの値は、0より大きい任意の整数に設定できます。値を0に設定すると、ネストされたオブジェクトはスキャンされません。</p> <p>デフォルト値：8</p>
[Endpoint. <tag>.]MailMaxLevel {integer}	<p>他のファイルが含まれる可能性のあるメーラーのファイル(pst、tbbなど)の最大ネスティングレベル(これらのファイルには他のファイルなどが含まれる場合もあります)。このパラメータの値は、ネスティングの上限を指定します。この上限を超えると、他のオブジェクト内のオブジェクトはスキャンされません。</p> <p>Endpoint. <tag>のプレフィックスが指定されている場合は、パラメータの値が <tag>接続ポイントにのみ設定されます。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。</p> <p>このパラメータの値は、0より大きい任意の整数に設定できます。値を0に設定すると、ネストされたオブジェクトはスキャンされません。</p> <p>デフォルト値：8</p>
[Endpoint. <tag>.]ContainerMaxLevel {integer}	<p>他のオブジェクトを含む他のタイプのオブジェクト(HTMLページやjarファイルなど)の最大ネスティングレベル。最大ネスティングレベルを超えると、オブジェクト内のオブジェクトはスキャンされません。</p> <p>Endpoint. <tag>のプレフィックスが指定されている場合は、パラメータの値が <tag>接続ポイントにのみ設定されます。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。</p> <p>このパラメータの値は、0より大きい任意の整数に設定できます。値を0に設定すると、ネストされたオブジェクトはスキャンされません。</p> <p>デフォルト値：8</p>
[Endpoint. <tag>.] MaxCompressionRatio {integer}	<p>圧縮されたオブジェクトの最大許容圧縮率(非圧縮サイズと圧縮サイズの比率)。オブジェクトの比率が制限を超えると、そのオブジェクトはスキャン中にスキップされます。</p> <p>圧縮率には2よりも小さい値は指定できません。</p> <p>デフォルト値：500</p>

コンポーネント構成の特別な側面

オプションのEndpoint. <tag>プレフィックスが付いているパラメータはグループ化できます。各グループは、クライアントがコンポーネントへの接続に使用する固有の接続ポイント(エンドポイント)を定義し、固有の<tag> IDが割り当てられています。同じグループに属するすべてのスキャンパラメータは、対応する接続ポイントに接続されているクライアントに対してデータがスキャンされる場合にのみ適用可能な設定を定義します。パラメータがEndpoint. <tag>のプレフィックスなしで指定されている場合は、すべての接続ポイントの値が設定されます。接続ポイントからパラメータを削除した場合は、このパラメータをプログラムのハードコードされたデフォルト値に戻す代わりに、同じ名前の対応する「親」パラメータの現在の値を使用します(Endpoint. <tag>プレフィックスなしで設定)。



ClamSocketパラメータは、リスニングソケットとこのソケットが対応するグループ(接続ポイント)の両方を定義するため、必ずEndpoint. <tag>プレフィックスを付けて指定する必要があります。

例

外部アプリケーション(サーバー)の2つのグループに対して2つの接続ポイントを設定する必要があります。グループをそれぞれ*servers1*と*servers2*と呼びます。また、*servers1*グループのサーバーはUNIXソケットを介して接続できるのに対し、*servers2*グループのサーバーはネットワーク接続を介して接続できます。さらに、ヒューリスティック解析はデフォルトで無効にする必要がありますが、*servers2*グループのサーバーには使用する必要があります。これを設定する方法を次の例で説明します。

- 1) **設定ファイル**を次のように編集します。

```
[ClamD]
HeuristicAnalysis = Off

[ClamD.Endpoint.servers1]
ClamSocket = /tmp/srv1.socket

[ClamD.Endpoint.servers2]
ClamSocket = 127.0.0.1:1234
HeuristicAnalysis = On
```

- 2) コマンドラインベース管理ツール**Dr.Web Ctl**では次のように設定します。

```
# drweb-ctl cfset ClamD.HeuristicAnalysis Off
# drweb-ctl cfset ClamD.Endpoint -a servers1
# drweb-ctl cfset ClamD.Endpoint -a servers2
# drweb-ctl cfset ClamD.Endpoint.servers1.ClamSocket /tmp/srv1.socket
# drweb-ctl cfset ClamD.Endpoint.servers2.ClamSocket 127.0.0.1:1234
# drweb-ctl cfset ClamD.Endpoint.servers2.HeuristicAnalysis On
```



どちらの方法でも効果は同じですが、設定ファイルを編集する場合は、drweb-configdコンポーネントにSIGHUP信号を送信して変更した設定を適用する必要があります(これを行うにはdrweb-ctl reload**コマンド**を発行します)。



外部アプリケーションとの統合

clamdインターフェースのエミュレーションにより、clamdアンチウイルスデーモン(ClamAVに含まれます)に接続可能な外部アプリケーションとDr.Web ClamDを統合できます。

以下の表は、アンチウイルススキャンにclamdを使用できるアプリケーションの例を示しています。

製品	統合
HTTPサービス	
HTTPプロキシサーバー Squid	clamdの使い方 インターネットから受信したファイルをスキャンする。 統合要件 中間コンポーネントとしてsquidclamavまたはHAVPを使用する。 ドキュメントへのリンク Squidのドキュメント: http://www.squid-cache.org/Doc/ squidclamavの説明とソースコードファイル: https://squidclamav.darold.net/
アンチウイルススキャン を実行できるHTTPプロ キシサーバー HAVP	clamdの使い方 インターネットから受信したファイルをスキャンする。 統合要件 アンチウイルススキャンにclamdを使用するようHAVPを設定する: <pre>ENABLECLAMD true CLAMDSOCKET <path_to_clamd_UNIX_socket></pre> または (UNIXソケットの代わりにTCP接続が使用されている場合): <pre>ENABLECLAMD true CLAMDSERVER <IP> CLAMDPORTR <port></pre> <path_to_clamd_UNIX_socket>または <IP>:<port>のペアは、Dr.Web ClamDで設定された接続ポイントのソケット (エンドポイント) に対応します。 ドキュメントへのリンク HAVPのドキュメント: http://www.havp.org/documentation/

clamdアンチウイルスデーモンと同様に、Dr.Web ClamDと直接通信する外部ソフトウェアコンポーネントの設定で、clamdに接続するためのアドレスをUNIXソケットへのパスとして、または設定された接続ポイント (エンドポイント) の1つでDr.Web ClamDにリスンされるTCPソケットとして指定します。



HAVPのDr.Web ClamDへの接続例:

1. Dr.Web ClamDの設定:

```
[ClamD]
Start = yes

[ClamD.Endpoint.proxy]
ClamdSocket = /var/run/drweb.clamd
```

2. HAVPの設定:

```
ENABLECLAMD true
CLAMDSOCKET /var/run/drweb.clamd
```

他のアンチウイルス製品への接続設定(ENABLE*パラメータ)はfalseに設定する必要があります。



Dr.Web File Checker

ファイルスキャンコンポーネントDr.Web File Checkerはファイルシステムのファイルとディレクトリをスキャンするように設計されており、Dr.Web for UNIX Internet Gatewaysの他のコンポーネントによってファイルシステムオブジェクトをスキャンするために使用されます。さらにこのコンポーネントは、隔離されたファイルが保存されているディレクトリの内容を管理するため、隔離マネージャーとしても機能します。

動作原理

このコンポーネントは、すべてのファイルシステムオブジェクト（ファイル、ディレクトリ、ブートレコード）へのアクセスに使用されます。スーパーユーザー（*root*）権限で起動します。

スキャン済みのすべてのファイルとディレクトリにインデックスを付け、特別なキャッシュに確認されたオブジェクトに関するすべてのデータを保存します。スキャン済みのオブジェクトやスキャン後変更されていないオブジェクトを繰り返しスキャンしないようにします（このようなオブジェクトに対するスキャンリクエストを受信した際は、キャッシュから取得した以前のスキャン結果が返されます）。

ファイルシステムオブジェクトを確認するリクエストがDr.Web for UNIX Internet Gatewaysのコンポーネントから受信されると、このオブジェクトにスキャンが必要かどうかを確認します。必要な場合は、[Dr.Web Scanning Engine](#)に対してスキャンタスクが生成されます。スキャンされたオブジェクトに脅威が含まれている場合、Dr.Web File Checkerはその脅威を検出された脅威レジストリに入れ、脅威への対応としてスキャンを開始したクライアントコンポーネントによって指定されている場合は駆除（修復、削除、または隔離）します。スキャンは、製品のさまざまなコンポーネントによって開始できます。

スキャン中、ファイルチェックコンポーネントでは、スキャン結果と適用されたアクションがあればそれを詳述するレポートを生成してクライアントコンポーネントに送信します。

標準のスキャン方法とは別に、内部使用には以下の特別な方法があります。

- 「*flow*」スキャン方法。このスキャン方法を使用するクライアントコンポーネントは、検出と駆除のパラメータを一度だけ初期化します。これらのパラメータは、このクライアントコンポーネントからのファイルをスキャンするための今後のすべてのリクエストに適用されます。
- 「*プロキシ*」スキャン方法。この方法を使用する場合、ファイルチェックコンポーネントは、検出された脅威にアクションを適用せずに、また今後のアクションを許可するために検出された脅威に関するレコードを保存せずに、ファイルをスキャンします。スキャン処理を開始したコンポーネントによって必要なアクションが適用される必要があります。この方法は[Dr.Web ClamD](#)コンポーネントによって使用されます。

[Dr.Web Ctl](#)ユーティリティの`flowscan`コマンド（`drweb-ctl`コマンドで起動）を使用し、「*フロー*」スキャン方法でファイルをスキャンできます。ただし、通常のオンデマンドスキャンでは`scan`コマンドを使用することを推奨しません。

作業中、ファイルスキャンコンポーネントは脅威のレジストリを保持して隔離を管理するだけでなく、ファイルスキャン全体の統計情報も収集し、最後の1分間、5分間、15分間の、1秒間に確認された平均ファイル数を計算します。



コマンドライン引数

Dr.Web File Checkerを起動するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-filecheck [<parameters>]
```

Dr.Web File Checkerは次のパラメータを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了します。 短縮形：-h 引数：なし
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了します。 短縮形：-v 引数：なし

例：

```
$ /opt/drweb.com/bin/drweb-filecheck --help
```

このコマンドは、Dr.Web File Checkerに関する簡単なヘルプ情報を出力します。

スタートアップノート

このコンポーネントは、自律モードで(他のコンポーネントから自律的に)OSのコマンドラインから直接起動することはできません。Dr.Web for UNIX Internet Gatewaysの他のコンポーネントからファイルシステムスキャンのリクエストを受信するときに、[Dr.Web ConfigD](#)設定デーモンによって自動的に起動されます。コンポーネントの動作を管理し、必要に応じてファイルをスキャンするには、Dr.Web for UNIX Internet Gateways用のコマンドラインベース管理ツール[Dr.Web Ctl](#)を使用できます([drweb-ctlコマンド](#)を使用して起動されます)。

Dr.Web File Checkerを使用して任意のファイルまたはディレクトリをスキャンするには、Dr.Web Ctlのscanコマンドを使用します。

```
$ drweb-ctl scan <path to file or directory>
```



コマンドラインから製品のこのコンポーネントに関するドキュメントを取得するには、`man 1 drweb-filecheck`コマンドを使用します。

設定パラメータ

コンポーネントは、Dr.Web for UNIX Internet Gatewaysの統合された[設定ファイル](#)の[FileCheck]セクションで指定されている設定パラメータを使用します。



このセクションは以下のパラメータを保存します。

パラメータ	説明
LogLevel <i>{logging level}</i>	コンポーネントの ロギングレベル 。 パラメータの値が指定されていない場合は、[Root] セクション の DefaultLogLevelパラメータの値が使用されます。 デフォルト値 : Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値 : Auto
ExePath <i>{path to file}</i>	コンポーネントの実行パス。 デフォルト値 : <opt_dir>/bin/drweb-filecheck <ul style="list-style-type: none">• GNU/Linuxの場合 : /opt/drweb.com/bin/drweb-filecheck• FreeBSDの場合 : /usr/local/libexec/drweb.com/bin/drweb-filecheck
DebugClientIpc <i>{Boolean}</i>	詳細なIPCメッセージをデバッグレベルでログファイルに含めるかどうかを示します (LogLevel = DEBUGの場合など)。 デフォルト値 : No
DebugScan <i>{Boolean}</i>	ファイルスキャン中に受信した詳細メッセージをデバッグレベルでログファイルに書き込みます (LogLevel = DEBUGの場合など)。 デフォルト値 : No
DebugFlowScan <i>{Boolean}</i>	「フロー」メソッドによるファイルスキャンに関する詳細メッセージをデバッグレベルでログファイルに書き込みます (LogLevel = DEBUGの場合など)。 デフォルト値 : No
DebugProxyScan <i>{Boolean}</i>	「プロキシ」メソッドによるファイルスキャンに関する詳細メッセージをデバッグレベルでログファイルに書き込みます (LogLevel = DEBUGの場合など)。通常、このスキャン方法は Dr.Web ClamD コンポーネントによって使用されます。 デフォルト値 : No
DebugCache <i>{Boolean}</i>	スキャンのキャッシュされた結果に関する詳細メッセージをデバッグレベルでログファイルに書き込みます (LogLevel = DEBUGの場合など)。 デフォルト値 : No
MaxCacheSize <i>{size}</i>	スキャンしたファイルに関するデータを保存するためのキャッシュの最大許容サイズ。 0を指定した場合、キャッシュは無効になります。 デフォルト値 : 50mb
RescanInterval <i>{time interval}</i>	前回のスキャンの結果がキャッシュ内にある場合にファイルが再スキャンされない期間 (保存された情報が最新のものと見なされる期間)。



パラメータ	説明
	<p>指定可能な値: 0秒 (0s) から1分 (1m) まで。 設定された間隔が1s未満の場合は遅延がないため、ファイルはリクエストに応じてスキャンされます。</p> <p>デフォルト値: 1s</p>
IdleTimeLimit <i>{time interval}</i>	<p>コンポーネントの最大アイドル時間。指定された時間が経過すると、コンポーネントはシャットダウンします。</p> <p>指定可能な値: 10秒 (10s) から30日 (30d) まで。 None値が設定されている場合、コンポーネントは永続的に機能します。コンポーネントがアイドル状態になると、SIGTERMシグナルは送信されません。</p> <p>デフォルト値: 30s</p>



Dr.Web Network Checker

ネットワークチェッカーエージェントDr.Web Network Checkerでは、ネットワーク経由で受信したデータをスキャンエンジンでスキャンできる他、分散ファイルでの脅威のスキャンを実行できます。このコンポーネントを使用すると、ネットワークホストを介してデータ(ファイルの内容など)を送受信できるようDr.Web for UNIX Internet Gatewaysがインストールされているネットワークホスト間の接続を調整し、スキャンを実行できます。このコンポーネントは、設定されているすべての利用可能なネットワークホストへのスキャンタスクの自動分配を(ネットワークを介して送受信することにより)調整します。このコンポーネントは、スキャンタスクによって生じる負荷をホスト間に分散させます。リモートホストとの接続が設定されていない場合、コンポーネントはすべてのデータをローカルのDr.Web Scanning Engineにのみ送信します。

このコンポーネントは、ネットワーク接続を介して受信したデータのスキャンに常に使用されます。したがって、コンポーネントが見つからないか使用できない場合、スキャン用にネットワーク接続を介してデータを送信するコンポーネント(Dr.Web ClamD、SpIDer Gate、Dr.Web ICAPD)のパフォーマンスは不正確になります。



このコンポーネントは、Dr.Web File Checkerコンポーネントを置き換えることができないため、ローカルファイルシステムにあるファイルの分散スキャンを整理するようには作られていません。ローカルファイルの分散スキャンを整理するには、[Dr.Web MeshD](#)コンポーネントを使用します。

ネットワークを介して転送されるデータのスキャンの負荷が高まると、利用できるファイル記述子の数が減少するため、スキャンに問題が生じる場合があります。この場合、Dr.Web for UNIX Internet Gatewaysに利用できるファイル記述子の[制限数を増やす](#)必要があります。

スキャン時には、SSL/TLSを適用することにより、オープンチャネル経由または保護されたチャネル経由のいずれかでデータを共有できます。安全なHTTPS接続を使用するには、ファイルを共有するホストに適切なSSLサーバー証明書とプライベートキーを提供する必要があります。SSLキーと証明書を生成するには、`openssl`ユーティリティを使用できます。`openssl`ユーティリティを使用して証明書とプライベートキーを生成する方法の例については、[付録E. SSL証明書を生成する](#)のセクションを参照してください。

動作原理

このコンポーネントにより、スキャンでローカルファイルシステムのファイルとして表されていないデータを[Dr.Web Scanning Engine](#)エンジン(ローカルまたはリモートホストにある)に送信できます。このデータは、(Dr.Web ICAPD、Dr.Web ClamD)接続を介してスキャンのデータを送信するコンポーネントによって処理されます。これらのコンポーネントは、ローカルホストにある場合でも、Dr.Web Scanning Engineエンジンへのファイル転送に常にDr.Web Network Checkerを使用することに注意してください。そのため、Dr.Web Network Checkerが利用できない場合、これらのコンポーネントは正しく機能しません。

また、Dr.Web Network Checkerにより、Dr.Web for UNIX Internet Gatewaysがインストールされているネットワーク(またはその他のDr.Web for UNIXソリューション10.1以降)の特定のノードセットとDr.Web for UNIX Internet Gatewaysを接続することで、ローカルファイルシステムでファイルとして表されない分散されたチェックデータの有無をまとめて確認できます。これによりこのコンポーネントは、検証でデータを交換する一連のネットワークノードであるスキャンクラスターを構築および設定できます(各インスタンスにDr.Web Network Checker分散検証エージェントの独自のインスタンスが必要です)。スキャンクラスターに含まれるネットワークの各ノードで、Dr.Web Network Checkerはスキャンデータのタスクの自動分散を実行し、接続が設定されているすべての使用可能なノードにネットワークを介して転送します。同時に、リモートノードで使用可能なリソースの量に応じて、データ検証によって発生するノードの負荷分散が実行されます(読み込みで使用可能なリソース量



の指標として、このノードのスキャンコアDr.Web Scanning Engineによって生成される子のスキャンプロセス数が使用されます)。使用されている各ノードでのチェックを待機しているファイルキューの長さも推定されます。

この場合、スキャンクラスタに含まれる任意のネットワークノードは、リモートスキャンにデータを送信するスキャンクライアントの他、検証のために指定されたネットワークノードからデータを受信するスキャンサーバーとして機能します。必要に応じて、ノードがスキャンサーバーまたはスキャンクライアントとしてのみ機能するように分散スキャンエージェントを設定できます。

スキャン用にネットワーク経由で受信したデータは、一時ファイルとしてローカルファイルシステムに保存され、[Dr.Web Scanning Engine](#)エンジンに送信されるか、利用できない場合はスキャンクラスタの他のノードに送信されます。

[設定](#)にあるInternalOnlyパラメータを使用すると、Dr.Web Network Checkerの動作モードを管理できます。これは、Dr.Web Network CheckerがDr.Web for UNIX Internet Gatewaysをスキャンクラスタに含めるために使用されるのか、Dr.Web for UNIX Internet Gatewaysローカルコンポーネントのみの内部目的のために使用されるのかを示します。



ファイルのチェック(スキャンクラスタのノードに対するスキャンジョブの分配を含む)にDr.Web Network Checkerを使用する独自のコンポーネント(外部アプリケーション)を作成できます。そのためDr.Web Network Checkerコンポーネントには、Google Protobufテクノロジーに基づくカスタムAPIが用意されています。Dr.Web Network Checker APIの他、Dr.Web Network Checkerを使用するクライアントアプリケーションのサンプルコードがdrweb-netcheckパッケージの一部として提供されています。

スキャンクラスタの作成例は、[スキャンクラスタの作成](#)セクションにあります。



コマンドライン引数

Dr.Web Network Checkerを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-netcheck [<parameters>]
```

Dr.Web Network Checkerは次のオプションを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了します。 短縮形：-h 引数：なし
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了します。 短縮形：-v 引数：なし

例：

```
$ /opt/drweb.com/bin/drweb-netcheck --help
```

このコマンドは、Dr.Web Network Checkerに関する簡単なヘルプ情報を出力します。

スタートアップノート

このコンポーネントは、自律モードで(他のコンポーネントから自律的に)OSのコマンドラインから直接実行することはできません。必要に応じて、[Dr.Web ConfigD](#)構成デーモンによって自動的に実行されます(通常はOSの起動時)。コンポーネント設定で、FixedSocketパラメータの値が指定されており、InternalOnlyパラメータがNoに設定されている場合、エージェントは常に実行されており、指定されたUNIXソケットを介してクライアントに使用可能です。ネットワーク経由でスキャンを開始するには、Dr.Web for UNIX Internet Gateways管理用の[Dr.Web Ctl](#)コマンドラインツールを使用できます(drweb-ctlコマンドで始まるもの)。リモートホストへの接続が設定されていない場合は、ローカルスキャンが開始されます。

Dr.Web Network Checkerを使用して任意のファイルまたはディレクトリをスキャンするには、Dr.Web Ctlツールのnetscanコマンドを使用します。

```
$ drweb-ctl netscan <path to file or directory>
```



コマンドラインから製品のこのコンポーネントに関するドキュメントを取得するには、`man 1 drweb-netcheck`コマンドを使用します。



設定パラメータ

このコンポーネントは、Dr.Web for UNIX Internet Gatewaysの統合された[設定ファイル](#)の[NetCheck]セクションで指定されている設定パラメータを使用します。

セクションには以下のパラメータが含まれています。

パラメータ	説明
LogLevel <i>{logging level}</i>	コンポーネントの ロギングレベル 。 パラメータの値が指定されていない場合は、[Root] セクション のDefaultLogLevelパラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行パス。 デフォルト値: <opt_dir>/bin/drweb-netcheck <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-netcheck• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-netcheck
FixedSocket <i>{path to file / address}</i>	固定されたDr.Web Network Checkerエージェントインスタンスのソケット。 このパラメータが指定されている場合、 Dr.Web ConfigD 設定デーモンは、このソケットを介してクライアントが使用可能な分散スキャンエージェントの実行中のコンポーネントのコピーが、常に存在することを確認します。 使用可能な値: <ul style="list-style-type: none">• <path to file>はローカルのUNIXソケットへのパスです。• <address>は、ペア <IP address>: <port>で示されるネットワークソケットです。 デフォルト値: (未設定)
InternalOnly <i>{Boolean}</i>	コンポーネントの動作モードの管理。 値がYesに設定されている場合、LoadBalance*設定やFixedSocketパラメータの値に関係なく、コンポーネントはDr.Web for UNIX Internet Gatewaysコンポーネントの内部目的にのみ使用され、スキャンクラスタへのDr.Web for UNIX Internet Gatewaysの組み込みや、外部(Dr.Web for UNIX Internet Gatewaysに対して)クライアントアプリケーションの処理には使用されません。 デフォルト値: No
RunAsUser <i>{UID / user name}</i>	その権限によりコンポーネントを実行するユーザーの名前。このユーザー名は、ユーザーのUIDまたはユーザーのログインとして指定できます。



パラメータ	説明
	<p>ユーザー名が数字で構成されている場合（つまりUIDに似ている場合）は、「name:」というプレフィックスを付けて指定します。たとえば、RunAsUser = name:123456です。</p> <p>ユーザー名が指定されていない場合、コンポーネント操作は開始後にエラーが発生して終了します。</p> <p>デフォルト値: drweb</p>
IdleTimeLimit <i>{time interval}</i>	<p>コンポーネントの最大アイドル時間。指定された値を超えると、コンポーネントはシャットダウンします。</p> <p>LoadBalanceAllowFromパラメータまたはFixedSocketパラメータが設定されている場合、この設定は無視されます（指定した時間を経過しても、コンポーネントは動作を終了しません）。</p> <p>指定可能な値: 10秒 (10s) から30日 (30d) まで。 None値が設定されている場合、コンポーネントは永続的に機能します。コンポーネントがアイドル状態になると、SIGTERMシグナルは送信されません。</p> <p>デフォルト値: 30s</p>
LoadBalanceUseSsl <i>{Boolean}</i>	<p>他のホストへの接続にSSL/TLSを使用します。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• Yes - SSL/TLSを使用します。• No - SSL/TLSを使用しません。 <p>このパラメータがYes値に設定されている場合、証明書と対応するプライベートキーを、このホストとこのホストがやり取りするホストに対して指定する必要があります（パラメータLoadBalanceSslCertificateおよびLoadBalanceSslKey）。</p> <p>デフォルト値: No</p>
LoadBalanceSslCertificate <i>{path to file}</i>	<p>安全なSSL/TLS接続を介して他のホストと通信するためにDr.Web Network Checkerによって使用されるSSL証明書へのパス。</p> <p>証明書ファイルとプライベートキーファイル（後述のパラメータで指定されます）は、一致するペアを形成する必要があります。</p> <p>デフォルト値: (未設定)</p>
LoadBalanceSslKey <i>{path to file}</i>	<p>安全なSSL/TLS接続を介して他のホストと通信するためにDr.Web Network Checkerによって使用されるプライベートキーへのパス。</p> <p>証明書ファイルとプライベートキーファイル（上記のパラメータで指定されます）は、一致するペアを形成する必要があります。</p> <p>デフォルト値: (未設定)</p>
LoadBalanceSslCa <i>{path}</i>	<p>信頼できるルート証明書のリストがあるディレクトリまたはファイルへのパス。これらの証明書には、SSL/TLSプロトコルを介してデータを交換するときにスキャンクラスタ内のエージェントが使用する、証明書の信頼性を証明する証明書が必要です。</p>



パラメータ	説明
	<p>パラメータ値が空の場合、このホストで動作しているDr.Web Network Checkerは、やり取りをするエージェントの証明書を認証しません。ただし設定によっては、ホスト上で動作しているエージェントが使用する証明書を、これらのエージェントが認証できます。</p> <p>デフォルト値：(未設定)</p>
LoadBalanceSslCrl <i>{path}</i>	<p>失効した証明書のシステムリストを含むディレクトリまたはファイルへのパス。</p> <p>パラメータ値が指定されていない場合、このホストで実行されているDr.Web Network Checkerは、やり取りするエージェントの証明書の有効性をチェックしません。ただし設定によっては、このホストで実行されているエージェントが使用する証明書の有効性をチェックする場合があります。</p> <p>デフォルト値：(未設定)</p>
LoadBalanceServerSocket <i>{address}</i>	<p>リモートホストからスキャン用に送信されたファイルを受信するために、Dr.Web Network Checkerがこのホスト上でリッスンしているネットワークソケット (IPアドレスとポート) (スキャンサーバーとして動作できる場合)。</p> <p>デフォルト値：(未設定)</p>
LoadBalanceAllowFrom <i>{IP address}</i>	<p>Dr.Web Network Checkerが (スキャンサーバーとして) スキャン用のファイルを受信するリモートネットワークホストのIPアドレス。</p> <p>リストをパラメータ値として指定できます。リストの値は、コンマ (引用符内の各値) で区切る必要があります。パラメータはセクションで複数回指定できます (この場合、そのすべての値が1つのリストにまとめられます)。</p> <p>例：ホストアドレス192.168.0.1と10.20.30.45のリストに追加します。</p> <p>1. 設定ファイルに値を追加します。</p> <ul style="list-style-type: none">• 1行に2つの値：<pre>[NetCheck] LoadBalanceAllowFrom = "192.168.0.1", "10.20.30.45"</pre>• 2行 (1行に1つの値)：<pre>[NetCheck] LoadBalanceAllowFrom = 192.168.0.1 LoadBalanceAllowFrom = 10.20.30.45</pre>



パラメータ	説明
	<p>2. drweb-ctl cfset コマンドを使用して値を追加します。</p> <pre data-bbox="703 293 1442 526"># drweb-ctl cfset NetCheck.LoadBalanceAllowFrom -a 192.168.0.1 # drweb-ctl cfset NetCheck.LoadBalanceAllowFrom -a 10.20.30.45</pre> <p>このパラメータが空の場合、削除されたファイルをスキャンのために受信することはできません(ホストはスキャンサーバーとして動作しません)。</p> <p>デフォルト値: (未設定)</p>
LoadBalanceSourceAddress <i>{IP address}</i>	<p>リモートスキャン用にファイルを転送するために、ホスト上のDr.Web Network Checkerによって使用されるネットワークインターフェースのIPアドレス(ホストがスキャンサーバーとして動作し、複数のネットワークインターフェースを持つ場合)。</p> <p>空の値を指定すると、OSカーネルによって自動的に選択されたネットワークインターフェースが使用されます。</p> <p>デフォルト値: (未設定)</p>
LoadBalanceTo <i>{address}</i>	<p>ホスト上のDr.Web Network Checkerが(ネットワークスキャンクライアントとして)リモートスキャン用のファイルを送信できるリモートホストのソケット(IPアドレスまたはポート)。</p> <p>リストをパラメータ値として指定できます。リストの値は、コンマ(引用符内の各値)で区切る必要があります。パラメータはセクションで複数回指定できます(この場合、そのすべての値が1つのリストにまとめられます)。</p> <p>例: ソケット192.168.0.1:1234および10.20.30.45:5678をリストに追加します。</p> <p>1. 設定ファイルに値を追加します。</p> <ul style="list-style-type: none">1つの文字列に2つの値: <pre data-bbox="703 1487 1442 1626">[NetCheck] LoadBalanceTo = "192.168.0.1:1234", "10.20.30.45:5678"</pre> <ul style="list-style-type: none">2つの文字列(文字列ごとに1つの値): <pre data-bbox="703 1682 1442 1821">[NetCheck] LoadBalanceTo = 192.168.0.1:1234 LoadBalanceTo = 10.20.30.45:5678</pre>



パラメータ	説明
	<p>2. <code>drweb-ctl cfset</code> コマンドを使用して値を追加します。</p> <pre># drweb-ctl cfset NetCheck.LoadBalanceTo -a 192.168.0.1:1234 # drweb-ctl cfset NetCheck.LoadBalanceTo -a 10.20.30.45:5678</pre> <p>パラメータ値が空の場合、ローカルファイルをリモートスキャン用に転送できません(ホストはネットワークスキャンクライアントとして動作しません)。</p> <p>デフォルト値：(未設定)</p>
<code>LoadBalanceStatusInterval</code> <i>{time interval}</i>	<p>ワークロードに関する情報を含む次のメッセージをすべてのスキャンクライアントに送信する際にホストによって考慮されるタイムインターバル (<code>LoadBalanceAllowFrom</code>パラメータで指定)。</p> <p>デフォルト値：1s</p>
<code>SpoolDir</code> <i>{path to directory}</i>	<p>スキャン用にネットワーク経由で送信され、Dr.Web Network Checkerによって受信されたファイルの保存に使用されるローカルファイルシステムのディレクトリ。</p> <p>デフォルト値：/tmp/netcheck</p>
<code>LocalScanPreference</code> <i>{fractional number}</i>	<p>ファイル(ローカルファイルまたはネットワーク経由で受信したファイル)をスキャンするスキャンサーバーが選択されたときに考慮される、ホストの相対的な重み(プライオリティ)。ローカル端末の相対的な重みが、スキャンサーバーとして利用可能なすべてのホストの重みよりも大きい場合、ファイルはローカルでスキャンされます。</p> <p>最小値：1</p> <p>デフォルト値：1</p>

スキャンクラスタの作成

このセクションの内容：

- [注意事項](#)
- [スキャンクラスタの作成例](#)
- [クラスタノードの設定](#)
- [クラスタの動作確認](#)

注意事項

ファイルや他のオブジェクトのスキャン中に分散チェックを実行できるスキャンクラスタを作成するには、各ノードにDr.Web Network Checkerコンポーネントがインストールされた一連のネットワークノードが必要です。クラスタノードにスキャン対象のデータの送受信以外の機能を持たせるには、ノードにスキャンエンジンDr.Web Scanning Engineもインストールする必要があります。そのため、スキャンクラスタのノードを作成するには、次のコンポーネントの最小セット(最低限のもの)をサーバーにインストールする必要があります(ここにリストされているコンポーネン

トの機能を保証するために自動的にインストールされるDr.Web for UNIX Internet Gatewaysの他のコンポーネントは、スキップされます。

1. Dr.Web Network Checker(`drweb-netcheck`パッケージ)は、ノード間のネットワークを提供するコンポーネントです。
2. **Dr.Web Scanning Engine**(`drweb-se`パッケージ)は、ネットワーク経由で受信したデータをスキャンするために必要なスキャンエンジンです。場合によっては、このコンポーネントが存在しません。その場合、ノードは他のスキャンクラスターノードに対してチェック対象のデータの送信のみを行います。

ピアツーピアネットワークのスキャンクラスターを構成するノード、つまり各ノードは、このノードのDr.Web Network Checkerコンポーネントで定義されている**設定**に応じて、スキャンクライアント(他のノードにスキャン用にデータを送信)またはスキャンサーバー(他のノードからスキャン用にデータを受信)として機能できます。適切に設定すれば、クラスターノードは同時にスキャンクライアントとスキャンサーバーの両方として機能します。

スキャンクラスター設定に関連するDr.Web Network Checkerのパラメータは、LoadBalanceで始まる名前を持ちます。

スキャンクラスターの作成例

下の図に表示されているスキャンクラスターの構成例を確認してください。

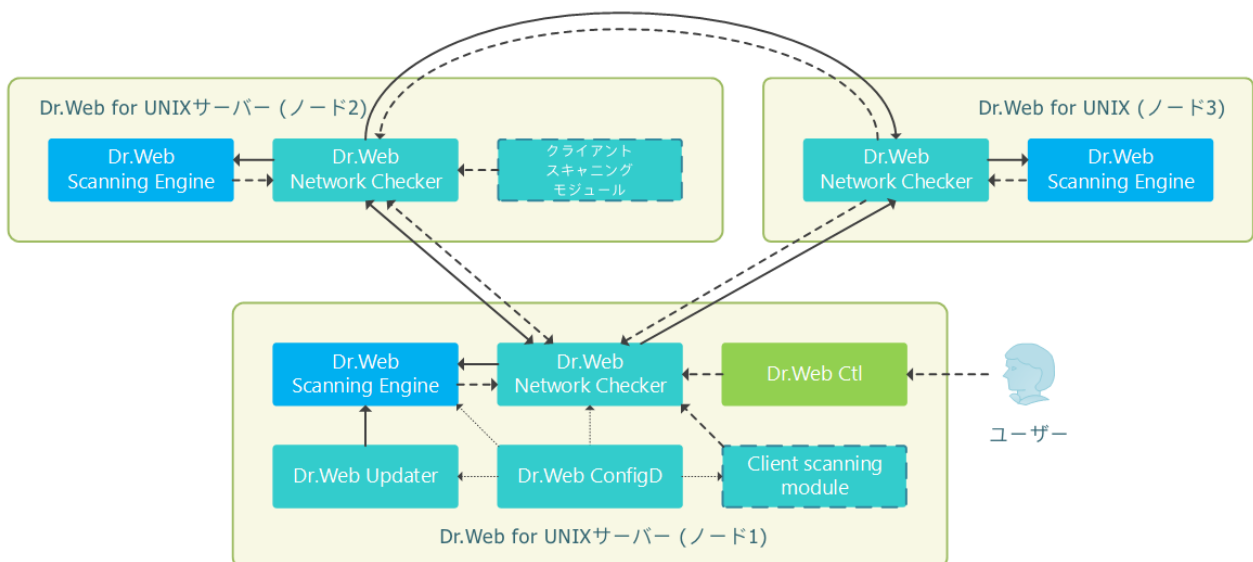


図 13. スキャンクラスターの構造

ここでは、クラスターは3つのノード(図ではノード1、ノード2、ノード3として表示)で構成されると想定します。この場合、ノード1とノード2は、UNIXサーバー用のDr.Webの上位製品がインストールされているサーバーです(Dr.Web for UNIX file serversまたはDr.Web for UNIXインターネットゲートウェイなど。製品タイプは不問)。ノード3は、ノード1とノード2から転送されたファイルのスキャンをサポートするためにのみ使用されます。したがって、必要最小限のコンポーネントセット(Dr.Web Network CheckerおよびDr.Web Scanning Engine)のみがインストールされます。ノードの操作性を確保するために自動的にインストールされる他のコンポーネント(Dr.Web ConfigDなど)は図に記載されていません。ノード1と2は、相互間でサーバーおよびスキャンクライアントの両方として機能し(スキャンに関連する負荷の相互分散を実行)、ノード3はサーバーとしてのみ機能し、ノード1と2からタスクを受信します。

これらのコンポーネントは、ローカルにインストールされたスキャンエンジンDr.Web Scanning Engineとクラスターパートナーノードの間で分散され、負荷分散に応じてスキャンサーバーとして機能します。



ローカルファイルシステムでファイルとして表されていないデータをスキャンするコンポーネントのみが、検証のクライアントモジュールとして機能することに注意してください。これは、SpIDer Guard ファイルシステムモニターおよびDr.Web File Checkerコンポーネントによるファイルの分散スキャンに使用できるスキャンクラスタを指します。

クラスタノードの設定

指定したクラスタ構成をカスタマイズするには、すべてのクラスタノードでDr.Web Network Checkerの設定を変更する必要があります。以下の設定はすべて.iniファイルで指定されます（設定ファイルの[フォーマット](#)の説明を参照）。

ノード1

```
[NetCheck]
InternalOnly=No
LoadBalanceUseSsl = No
LoadBalanceServerSocket = <Node 1 IP address>: <Node 1 port>
LoadBalanceAllowFrom = <Node 2 IP address>
LoadBalanceSourceAddress = <Node 1 IP address>
LoadBalanceTo = <Node 2 IP address>: <Node 2 port>
LoadBalanceTo = <Node 3 IP address>: <Node 3 port>
```

ノード2

```
[NetCheck]
InternalOnly=No
LoadBalanceUseSsl = No
LoadBalanceServerSocket = <Node 2 IP address>: <Node 2 port>
LoadBalanceAllowFrom = <Node 1 IP address>
LoadBalanceSourceAddress = <Node 2 IP address>
LoadBalanceTo = <Node 1 IP address>: <Node 1 port>
LoadBalanceTo = <Node 3 IP address>: <Node 3 port>
```

ノード3

```
[NetCheck]
InternalOnly=No
LoadBalanceUseSsl = No
LoadBalanceServerSocket = <Node 3 IP address>: <Node 3 port>
LoadBalanceAllowFrom = <Node 1 IP address>
LoadBalanceAllowFrom = <Node 2 IP address>
```

注意:

- 他の(ここに記載されていない)Dr.Web Network Checkerパラメータは変更されません。
- IPアドレスとポート番号は実際のものに変更する必要があります。
- この例では、ノード間のデータ交換におけるSSLの使用は無効になっています。SSLを使用する必要がある場合は、LoadBalanceUseSslパラメータに値Yesを設定するとともに、パラメータ



LoadBalanceSslCertificate、LoadBalanceSslKey、LoadBalanceSslCaに必要な値を設定する必要があります。

クラスタの動作確認

データディストリビューションモードでのクラスタの動作を確認するには、ノード1とノード2で次のコマンドを使用します。

```
$ drweb-ctl netscan <path to file or directory>
```

指定されたコマンドを実行するときは、指定されたディレクトリのファイルをDr.Web Network Checkerでチェックする必要があります。これにより、カスタマイズされたクラスタノードにチェックが分散されます。スキャン前に各ノードのネットワークチェックの統計を表示するには、次のコマンドを使用してDr.Web Network Checkerの統計の表示を実行します（統計の表示を中断するにはCTRL+Cを押します）。

```
$ drweb-ctl stat -n
```



Dr.Web Scanning Engine

Dr.Web Scanning Engineスキャンエンジンでは、ディスクデバイスのファイルやブートレコード (*MBR* - マスターブートレコード、*VBR* - ボリュームブートレコード) に含まれている、ウイルスなどの悪意のあるオブジェクトを検索できます。このコンポーネントはスキャンエンジンDr.Web Virus-Finding Engineをメモリに読み込んで起動する他、このエンジンが脅威の検出のために使用するDr.Webウイルスデータベースの読み込みも行います。

このスキャンエンジンは、Dr.Web for UNIX Internet Gatewaysの他のコンポーネント (Dr.Web File CheckerとDr.Web Network Checker、部分的にはDr.Web MeshD) からスキャンリクエストを受信するサービスとして、デーモンモードで動作します。Dr.Web Scanning EngineとDr.Web Virus-Finding Engineが存在しないか使用できない場合、このノードではアンチウイルススキャンは実行されません (ただし、Dr.Web MeshDコンポーネントを含むDr.Web for UNIX Internet Gatewaysを除きます。このコンポーネントの設定には、スキャンエンジンサービスを提供するローカルクラウドノードへの接続が含まれています)。

動作原理

このコンポーネントは、埋め込まれた脅威についてファイルシステムオブジェクト (ファイルおよびブートディスクレコード) をスキャンするリクエストを、Dr.Web for UNIX Internet Gatewaysのコンポーネントから受信するサービスとして動作します。また、スキャンタスクをキューに入れ、リクエストされたオブジェクトをDr.Web Virus-Finding Engineスキャンエンジンを使用してスキャンします。脅威が検出され、スキャンタスクによって脅威を修復するように指示があった場合、スキャンされたオブジェクトにこのアクションを適用できるのであれば、スキャンエンジンは修復を試みます。

スキャンエンジン、Dr.Web Virus-Finding Engineスキャンエンジン、およびウイルスデータベースは1つの単位を構成しており、分離することはできません。スキャンエンジンはウイルスデータベースをダウンロードし、クロスプラットフォームのスキャンエンジンDr.Web Virus-Finding Engineの動作環境を提供します。ウイルスデータベースとスキャンエンジンは、Dr.Web for UNIX Internet Gatewaysに含まれている**Dr.Web Updater**更新コンポーネントによって更新されますが、このコンポーネントはスキャンエンジンの一部ではありません。対応するコマンドがユーザーから送信された場合、更新コンポーネントは**Dr.Web ConfigD**設定デーモンによって定期的または強制的に実行されます。さらに、Dr.Web for UNIX Internet Gatewaysが集中管理モードで動作している場合、ウイルスデータベースとスキャンエンジンの更新は**Dr.Web ES Agent**によって実行されます。後者のコンポーネントは集中保護サーバーとやり取りし、更新を受け取ります。

Dr.Web Scanning Engineは設定デーモンDr.Web ConfigDの管理下でも、自律モードでも動作できます。前者の場合、デーモンはエンジンを実行し、アンチウイルスデータベースが最新であることを確認します。後者の場合、エンジンの起動とウイルスデータベースの更新は、このエンジンを使用する外部アプリケーションによって実行されます。ファイルのスキャンを要求するスキャンエンジンにリクエストを発行するDr.Web for UNIX Internet Gatewaysのコンポーネントは、他の外部アプリケーションと同じインターフェースを使用します。



ユーザーは、ファイルのチェックのためにDr.Web Scanning Engineを使用する独自のコンポーネント (外部アプリケーション) を作成できます。このため、Dr.Web Scanning EngineにはGoogle Protobufに基づく特別なAPIが含まれています。Dr.Web Scanning Engine APIガイドと、Dr.Web Scanning Engineを使用したクライアントアプリケーションの例を入手するには、Doctor Webパートナーケア部門 (<https://partners.drweb.com/>) にお問い合わせください。

受信したタスクは、優先度 (高い、通常、低い) ごとのキューに自動的に分配されます。キューの選択は、タスクを作成したコンポーネントによって異なります。たとえば、ファイルシステムモニターによって作成されたタスクは、応答時間がモニターにとって重要であるため、優先順位が高くなります。スキャンエンジンは、スキャン用に受信したすべてのタスクの数やキューの長さなど、操作に関わる統計を計算します。平均負荷率として、スキャンエンジン



は1秒あたりのキューの平均長を使用します。このレートは、直近1分間、直近5分間、直近15分間の平均です。

Dr.Web Virus-Finding Engineスキャンエンジンは、機械語の命令やその他の実行可能コードの属性に基づいて潜在的に危険なオブジェクトを検出するために設計された、シグネチャ解析(シグネチャベースの脅威の検出)やその他のヒューリスティック解析および動作解析の[方法](#)をサポートしています。



ヒューリスティック解析は信頼性の高い結果を保証できず、次のようなエラーが発生する可能性があります。

- **最初のタイプのエラー。**これらのエラーは、安全なオブジェクトが悪意のあるものとして検出された場合に発生します(誤検知)。
- **2番目のタイプのエラー。**これらのエラーは、悪意のあるオブジェクトが安全であると検出されたときに発生します。

したがって、ヒューリスティックアナライザによって検出されたオブジェクトは**疑わしいもの**として扱われます。

疑わしいオブジェクトは隔離に移動することをお勧めします。ウイルスデータベースを更新した後、そのようなファイルはシグネチャ解析を使用してスキャンできます。2番目のタイプのエラーを避けるには、ウイルスデータベースを最新の状態に保ってください。

Dr.Web Virus-Finding Engineスキャンエンジンを使用すると、ファイルと圧縮されたオブジェクトの両方、または異なるコンテナ内のオブジェクト(アーカイブやメールメッセージなど)をスキャンして修復できます。

コマンドライン引数

スキャンエンジンDr.Web Scanning Engineをコマンドラインから実行するには、次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-se <socket> [<parameters>]
```

必須の<socket>引数は、クライアントコンポーネントの要求を処理するためにDr.Web Scanning Engineによって使用されるソケットのアドレスを示します。ファイルパス(UNIXソケット)としてのみ設定できます。

Dr.Web Scanning Engineは次のオプションを処理できます。

パラメータ	説明
--help	機能: コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了します。 短縮形: -h 引数: なし
--version	機能: このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了します。 短縮形: -v 引数: なし。

追加の起動パラメータ(設定ファイルのパラメータと同じものであり、必要に応じて置き換えます)。



<code>--CoreEnginePath</code>	<p>機能：Dr.Web Virus-Finding Engineスキャンエンジンのライブラリへのパスを指定します。</p> <p>短縮形：なし。</p> <p>引数：<path to the file> - 使用するライブラリへのフルパス。</p>
<code>--VirusBaseDir</code>	<p>機能：ウイルスデータベースファイルがあるディレクトリへのパスを指定します。</p> <p>短縮形：なし。</p> <p>引数：<path to the directory> - ウイルスデータベースディレクトリへのパス。</p>
<code>--TempDir</code>	<p>機能：一時ファイルがあるディレクトリへのパスを指定します。</p> <p>短縮形：なし。</p> <p>引数：<path to the directory> - 一時ファイルを含むディレクトリへのフルパス。</p>
<code>--Key</code>	<p>機能：キーファイルへのパスを指定します。</p> <p>短縮形：なし。</p> <p>引数：<path to the file> - 使用するキーファイルへのフルパス。</p>
<code>--MaxForks</code>	<p>機能：スキャン中にDr.Web Scanning Engineによって起動できる子プロセスの最大許容数を指定します。</p> <p>短縮形：なし。</p> <p>引数：<number> - 子プロセスの最大許容数。</p>
<code>--WatchdogInterval</code>	<p>説明：Dr.Web Scanning Engineが、子プロセスが動作可能かどうかをチェックし、応答を停止したプロセスを停止する頻度。</p> <p>短縮形：なし。</p> <p>引数：<time interval> - 子プロセスをチェックする頻度。</p>
<code>--Shelltrace</code>	<p>機能：シエルトレースをオンにします (Dr.Web Virus-Finding Engineによって実行されたファイルスキャンの詳細情報をログに記録します)。</p> <p>短縮形：なし。</p> <p>引数：なし。</p>
<code>--LogLevel</code>	<p>説明：動作中にDr.Web Scanning Engineによって実行されるロギングのレベルを設定します。</p> <p>短縮形：なし。</p> <p>引数：<logging level>。使用可能な値：</p> <ul style="list-style-type: none">• DEBUG - 最も詳細なロギングレベル。すべてのメッセージとデバッグ情報が登録されます。• INFO - すべてのメッセージが登録されます。• NOTICE - すべてのエラーメッセージ、警告、通知が登録されます。• WARNING - すべてのエラーメッセージと警告が登録されます。• ERROR - エラーメッセージのみが登録されます。
<code>--Log</code>	<p>説明：コンポーネントメッセージのロギングの方法を指定します。</p> <p>短縮形：なし。</p> <p>引数：<log type>。使用可能な値：</p> <ul style="list-style-type: none">• <code>Stderr[:ShowTimestamp]</code> - メッセージは標準エラーestreamの<code>stderr</code>に出力されます。 追加オプション<code>ShowTimestamp</code>は、すべてのメッセージにタイムスタンプを追加するために使用します。• <code>Syslog[:<facility>]</code> - メッセージはシステムロギングサービス<code>syslog</code>に送信されます。



追加オプション *<facility>* は、syslogのメッセージ登録レベルを指定するために使用します。次の値を使用できます。

- DAEMON - デーモンのメッセージ。
- USER - ユーザープロセスのメッセージ。
- MAIL - メールプログラムのメッセージ。
- LOCAL0 - ローカルプロセス0のメッセージ。

...

- LOCAL7 - ローカルプロセス7のメッセージ。

- *<path>* - すべてのメッセージが登録されているファイルへのパス。

例：

```
--Log /var/opt/drweb.com/log/se.log
--Log Stderr:ShowTimestamp
--Log Syslog:DAEMON
```

例：

```
$ /opt/drweb.com/bin/drweb-se /tmp/drweb.ipc/.se --MaxForks=5
```

このコマンドはDr.Web Scanning Engineスキャンエンジンのインスタンスを起動し、クライアントコンポーネントとのインタラクション用の/tmp/drweb.ipc/.se UNIXソケットを作成し、子スキャンプロセスの数を5つに制限します。

スタートアップノート

必要に応じて、Dr.Web Scanning Engineスキャンエンジンのインスタンスはいくつでも起動できます。インスタンスは、(Dr.Web for UNIX Internet Gatewaysのコンポーネントだけでなく)クライアントアプリケーションにもスキャンサービスを提供します。その場合、コンポーネントの**設定**でFixedSocketPathパラメータの値が指定されていると、スキャンエンジンの1つのインスタンスが**Dr.Web ConfigD**設定デーモンによって常に実行され、このUNIXソケットを介してクライアントから常に利用可能になります。コマンドラインから直接起動したスキャンエンジンのインスタンスは、設定デーモンが実行中であっても、設定デーモンへの接続を確立せずに自律モードで動作します。コンポーネントの動作を管理し、必要に応じてファイルをスキャンするには、Dr.Web for UNIX Internet Gatewaysのコマンドラインベース管理ツール**Dr.Web Ctl**を使用できます(drweb-ctl **コマンド**を使用して起動します)。

Dr.Web Scanning Engineを使用して任意のファイルまたはディレクトリをスキャンするには、Dr.Web Ctlツールのrawscanコマンドを使用します。

```
$ drweb-ctl rawscan <path to file or directory>
```



コマンドラインから製品のこのコンポーネントに関するドキュメントを取得するには、`man 1 drweb-se`コマンドを使用します。



設定パラメータ

このコンポーネントは、Dr.Web for UNIX Internet Gatewaysの統合された[設定ファイル](#)の [ScanEngine] セクションで指定されている設定パラメータを使用します。

このセクションは以下のパラメータを保存します。

パラメータ	説明
LogLevel <i>{logging level}</i>	コンポーネントの ロギングレベル 。 パラメータの値が指定されていない場合は、[Root] セクション の DefaultLogLevelパラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行パス。 デフォルト値: <opt_dir>/bin/drweb-se <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-se• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-se
FixedSocketPath <i>{path to file}</i>	Dr.Web Scanning Engineスキャンエンジンの固定インスタンスのUNIXソケットへのパス。 このパラメータが指定されている場合、 Dr.Web ConfigD 設定デーモンは、このソケットを介してクライアントが使用可能なスキャンエンジンのコンポーネントのコピーが常に実行されていることを確認します。 デフォルト値: (未設定)
IdleTimeLimit <i>{time interval}</i>	コンポーネントの最大アイドル時間。指定された時間が経過すると、コンポーネントはシャットダウンします。 FixedSocketPathパラメータが設定されている場合、この設定は無視されません(指定した時間を経過しても、コンポーネントは動作を終了しません)。 指定可能な値: 10秒 (10s) から30日 (30d) まで。 None値が設定されている場合、コンポーネントは永続的に機能します。コンポーネントがアイドル状態になると、SIGTERMシグナルは送信されません。 デフォルト値: 1h
MaxForks <i>{integer}</i>	同時に実行できる、Dr.Web Scanning Engineによって実行される子プロセスの最大許容数。 デフォルト値: 使用可能なCPUコアの2倍の数が自動的に使用されます。算出された数が4未満の場合は4になります。
BufferedIo <i>{On / Off}</i>	ファイルをスキャンするときは、バッファ付き入出力 (I/O) を使用します。 FreeBSDおよびGNU/Linux OSでバッファ付きI/Oを使用すると、低速ディスクでのファイルスキャン速度を上げることができます。



パラメータ	説明
	デフォルト値 : Off
WatchdogInterval {time interval}	応答を停止したプロセス(「watchdog」)を検出するために、子プロセスが動作可能かどうかをDr.Web Scanning Engineがチェックする頻度。 デフォルト値 : 1.5s



Dr.Web Updater

更新コンポーネントのDr.Web Updaterは、Doctor Web更新サーバーからウイルスデータベースおよびDr.Web Virus-Finding Engineスキャンエンジンの利用可能な更新をすべて受信し、更新をDr.Web for UNIX製品コンポーネントのローカルクラウドと([Dr.Web MeshD](#)が製品に含まれている場合はそれを経由して)同期させることを目的に設計されています。

Dr.Web for UNIX Internet Gatewaysが[集中管理モード](#)で動作している場合、更新は集中管理サーバー(Dr.Web Enterprise Serverなど)から受信されます。その場合、すべての更新は[Dr.Web ES Agent](#)経由でサーバーから受信され、Dr.Web Updaterは更新のダウンロードには使用されません(Dr.Web for UNIX製品のローカルクラウドと更新が同期されることはありません)。

動作原理

このコンポーネントは、Doctor Web更新サーバーへの接続を確立して、ウイルスデータベースとDr.Web Virus-Finding Engineスキャンエンジン、Webリソースカテゴリーのデータベースの更新がないか確認することを目的に設計されています。利用可能な更新ゾーンを構成するサーバーのリストは、特別なファイルに保存されます(ファイルは改変を防ぐために署名されています)。Doctor Web更新サーバーへの接続では、基本認証とダイジェスト認証のみがサポートされています。

Dr.Web for UNIX Internet Gatewaysが集中管理サーバーに接続されていない場合、またはモバイルモードでサーバーに接続されている場合、Dr.Web UpdaterはDr.Web ConfigD設定デーモンによって自動的に起動されます。起動は、[設定](#)で指定された周期で実行されます。適切な[コマンド](#)をユーザーから受け取った場合、このコンポーネントは設定デーモンによって起動することもできます(スケジュールされていない更新)。

サーバー上で利用可能になった更新は、`<var_dir>/cache`ディレクトリ(GNU/Linuxの場合は`var/opt/drweb.com/cache`)にダウンロードされ、その後Dr.Web for UNIX Internet Gatewaysの作業ディレクトリに移されます。

デフォルトでは、更新はすべてDr.Webの全製品に共通の更新ゾーンから実行されます。更新ゾーンに含まれる、デフォルトで使用されるサーバーのリストは、`*Dr1Dir`パラメータで定義されたディレクトリにあるファイルで指定され、更新タイプ別にグループ化されています(ウイルスデータベースおよびスキャンエンジンと、Webリソースカテゴリーのデータベース)。これらのファイルは、更新されたコンポーネント(ウイルスデータベース、スキャンエンジン、アンチスパムコンポーネント)によってグループ化されています。ユーザーのリクエストに応じて(更新タイプごとに)特別な更新ゾーンを作成できます。これが、`*CustomDr1Dir`パラメータで指定されたディレクトリにある、別のファイル(デフォルト名は`custom.dr1`)で指定されているサーバーリストです。この場合、更新コンポーネントは、デフォルトゾーンのサーバーを使用せずに、これらのサーバーからのみ更新を受信します。

特別な更新ゾーンを使用しない場合は、コンポーネント設定で該当するパラメータの`*CustomDr1Dir`値を削除します。



サーバーリストを含むファイルの中身は署名されているため、ファイルを変更することはできません。更新サーバーの特別なリストを作成する必要がある場合は、[テクニカルサポート](#)にお問い合わせください。

このコンポーネントは、ユーザーが次に更新のロールバックをリクエストする場合に備えて、更新したファイルをバックアップできます。バックアップするファイルの場所と詳細レベルは設定で指定できます。更新をロールバックするに



は、Dr.Web Ctl [Dr.Web Ct](#)コマンドラインからソリューションを管理するDr.Web for UNIX Internet Gateways用のコマンドラインツールを使用します (drweb-ctlコマンドで実行されます)。

Dr.Web for UNIX Internet GatewaysがDr.Web for UNIX製品のローカルクラウドに接続されていて、集中管理サーバーに接続されていない場合、Dr.Web Updaterコンポーネントは、クラウドホストによって受信された更新の同期にも使用されます。つまり、更新サーバーが受信した更新をクラウドに送信し、クラウドから更新を受信することになるため、Dr.Web更新サーバーの総負荷を軽減できます。このオプションはコンポーネントの[設定](#)で有効または無効にできます。

コマンドライン引数

Dr.Web Updaterを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-update [<parameters>]
```

Dr.Web Updaterは次のオプションを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了します。 短縮形：-h 引数：なし
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了します。 短縮形：-v 引数：なし

例：

```
$ /opt/drweb.com/bin/drweb-update --help
```

このコマンドは、Dr.Web Updaterに関する簡単なヘルプ情報を出力します。

スタートアップノート

このコンポーネントは、自律モードで(他のコンポーネントから自律的に)OSのコマンドラインから直接起動することはできません。必要に応じて[Dr.Web ConfigD](#)設定デーモンによって自動的に起動されます。コンポーネントの動作を管理し、ウイルスデータベースとスキャンエンジンを更新するには、Dr.Web for UNIX Internet Gateways用のコマンドラインベース管理ツール[Dr.Web Ct](#)を使用できます(これはdrweb-ctl[コマンド](#)を使用して呼び出されます)。



コマンドラインから製品のこのコンポーネントに関するドキュメントを取得するには、`man 1 drweb-update`コマンドを使用します。



設定パラメータ

このコンポーネントは、Dr.Web for UNIX Internet Gatewaysの統合された[設定ファイル](#)の[Update]セクションで指定されている設定パラメータを使用します。

セクションには以下のパラメータが含まれています。

パラメータ	説明
LogLevel <i>{logging level}</i>	コンポーネントの ロギングレベル 。 パラメータの値が指定されていない場合は、[Root] セクション のDefaultLogLevelパラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行パス。 デフォルト値: <opt_dir>/bin/drweb-update <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-update• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-update
RunAsUser <i>{UID user name}</i>	このパラメータは、コンポーネントを実行するユーザー名を決定します。ユーザー名は、ユーザーのUIDまたはユーザーのログインとして指定できます。ユーザー名が数字で構成されている場合(つまりUIDに似ている場合は)、「name:」というプレフィックスを付けて指定します。たとえば、RunAsUser = name:123456です。 ユーザー名が指定されていない場合、コンポーネント操作は開始後にエラーが発生して終了します。 デフォルト値: drweb
UpdateInterval <i>{time interval}</i>	Dr.Web更新サーバーで更新を確認する頻度。これは、(自動または手動で開始した)更新サーバーへの接続が成功してから次に更新の実行を試みるまでの時間間隔です。 デフォルト値: 30m
RetryInterval <i>{time interval}</i>	前回の試行が失敗した場合に、更新サーバーを使用して更新の実行を再試行する頻度。 指定可能な値: 1分(1m)から30分(30m)まで。 デフォルト値: 3m
MaxRetries <i>{integer}</i>	前回の試行が失敗した場合に、更新サーバーを使用して(RetryIntervalで指定された頻度で)更新の実行を繰り返し試みる回数。 値が0に設定されている場合、試行は繰り返されません(次の更新は、UpdateIntervalで指定された時間を経過した後に実行されます)。



パラメータ	説明
Proxy <i>{connection string}</i>	<p>デフォルト値: 3</p> <p>Dr.Web更新サーバーへの接続時にアップデーターコンポーネント (Dr.Web Updater) が使用するプロキシサーバーに接続するためのパラメータを保存します (外部サーバーへの直接接続がネットワークのセキュリティポリシーによって禁止されている場合など)。</p> <p>パラメータ値が指定されていない場合、プロキシサーバーは使用されません。</p> <p>使用可能な値:</p> <p><connection string>は、プロキシサーバーの接続文字列です。文字列のフォーマット (URL) は以下のとおりです。</p> <pre>[<protocol>://] [<user>: <password>@] <host>: <port></pre> <p>各パラメータは次のとおりです。</p> <ul style="list-style-type: none">• <protocol>は、使用されるプロトコルタイプです (現在のバージョンでは、httpのみが使用可能です)。• <user>は、プロキシサーバーに接続するためのユーザー名です。• <password>は、プロキシサーバーに接続するためのパスワードです。• <host>は、プロキシのホストアドレスです (IPアドレスまたはドメイン名、つまりFQDN)。• <port>は使用するポートです。 <p>URLの <protocol>および <user>: <password>の部分がありません。プロキシサーバーのアドレス <host>: <port>は必須です。</p> <p>ユーザー名またはパスワードに「@」、「%」、「:」の文字が含まれている場合、これらの文字はそれぞれ「%40」、「%25」、「%3A」の16進コードに変更する必要があります。</p> <p>例:</p> <ol style="list-style-type: none">1. 設定ファイルでの設定。<ul style="list-style-type: none">• ポート123を使用した proxyhost.company.org でホストされているプロキシサーバーへの接続: Proxy = proxyhost.company.org:123• ポート3336を使用し、パスワードが「passw」のユーザー「legaluser」としてHTTPプロトコルを経由した 10.26.127.0 でホストされているプロキシサーバーへの接続: Proxy = http:// legaluser:passw@10.26.127.0:3336• ポート3336、ユーザー名「user@company.com」、パスワード「passw%123:」を使用した 10.26.127.0 でホストされているプロキシサーバーへの接続: Proxy = user%40company.com:passw%25123%3A@10.26.127.0:3336



パラメータ	説明
	<p>2. drweb-ctl cfset コマンドを使用して、同じ値を設定する。</p> <pre data-bbox="635 295 1439 528"># drweb-ctl cfset Update.Proxy proxyhost.company.org:123 # drweb-ctl cfset Update.Proxy http://legaluser:passw@10.26.127.0:3336 # drweb-ctl cfset Update.Proxy user% 40company.com:passw%25123%3A@10.26.127.0:3336</pre> <p>デフォルト値：(未設定)</p>
ExcludedFiles <i>{file name}</i>	<p>Dr.Web Updaterコンポーネントによって更新されないファイルの名前を定義します。</p> <p>リストをパラメータ値として指定できます。リストの値は、コンマ(引用符内の各値)で区切る必要があります。パラメータはセクションで複数回指定できます(この場合、そのすべての値が1つのリストにまとめられます)。</p> <p>例：以下のファイルをリストに追加します。123.vdbおよび456.dws。</p> <ol style="list-style-type: none">設定ファイルに値を追加します。<ul style="list-style-type: none">1つの文字列に2つの値：<pre data-bbox="635 945 1439 1048">[Update] ExcludedFiles = "123.vdb", "456.dws"</pre>2つの文字列(文字列ごとに1つの値)：<pre data-bbox="635 1111 1439 1245">[Update] ExcludedFiles = 123.vdb ExcludedFiles = 456.dws</pre>drweb-ctl cfset コマンドを使用して値を追加します。<pre data-bbox="635 1308 1439 1473"># drweb-ctl cfset Update.ExcludedFiles -a 123.vdb # drweb-ctl cfset Update.ExcludedFiles -a 456.dws</pre> <p>デフォルト値：drweb32.lst</p>
NetworkTimeout <i>{time interval}</i>	<p>更新プロセス中にUpdaterコンポーネントのネットワーク関連の動作に課されるタイムアウト時間。</p> <p>このパラメータは、接続が一時的に切断されたときに使用されます。タイムアウトが切れる前に接続が再度確立された場合、中断された更新プロセスが続行されます。</p> <p>75sを超えるタイムアウト値を指定した場合は、TCPタイムアウトによって接続が閉じられるため効力を持ちません。</p> <p>最小値：5s</p> <p>デフォルト値：60s</p>



パラメータ	説明
BaseDrlDir <i>{path to directory}</i>	<p>標準的な更新ゾーンの更新サーバーへの接続に使用されるファイルを含むディレクトリへのパスを定義します。更新コンポーネントがウイルスデータベースおよびスキャンエンジンを更新するために使用されます。</p> <p>デフォルト値: <var_dir>/drl/bases</p> <ul style="list-style-type: none">• GNU/Linuxの場合: /var/opt/drweb.com/drl/bases• FreeBSDの場合: /var/drweb.com/drl/bases
BaseCustomDrlDir <i>{path to directory}</i>	<p>特別な「カスタマイズされた」更新ゾーンへの接続に使用されるファイルを含むディレクトリへのパスを定義します。ウイルスデータベースとスキャンエンジンを更新するために使用されます。</p> <p>パラメータで定義されたディレクトリ内に、空でない署名付きサーバーリストファイル(.drlファイル)がある場合、更新はこれらのサーバーからのみ実行され、主要なゾーンサーバー(上記を参照)はウイルスデータベースおよびスキャンエンジンの更新には使用されません。</p> <p>デフォルト値: <var_dir>/custom-drl/bases</p> <ul style="list-style-type: none">• GNU/Linuxの場合: /var/opt/drweb.com/custom-drl/bases• FreeBSDの場合: /var/drweb.com/custom-drl/bases
BaseUpdateEnabled <i>{Boolean}</i>	<p>ウイルスデータベースとスキャンエンジンの更新が許可されているかどうかを示すインジケータ。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• Yes - 更新は許可されており、実行されます。• No - 更新は許可されていないため実行されません。 <p>デフォルト値: Yes</p>
VersionDrlDir <i>{path to directory}</i>	<p>サーバーへの接続に使用されるファイルを含むディレクトリへのパスを定義します。Dr.Web for UNIX Internet Gatewaysのバージョンの更新に使用されます。</p> <p>デフォルト値: <var_dir>/drl/version</p> <ul style="list-style-type: none">• GNU/Linuxの場合: /var/opt/drweb.com/drl/version• FreeBSDの場合: /var/drweb.com/drl/version
VersionUpdateEnabled <i>{Boolean}</i>	<p>Dr.Web for UNIX Internet Gatewaysコンポーネントのバージョンの更新が許可されているかどうかを示すインジケータ。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• Yes - 更新は許可されており、実行されます。• No - 更新は許可されていないため実行されません。 <p>デフォルト値: Yes</p>
DwsCustomDrlPath <i>{path to file}</i>	<p>特別な更新ゾーンのサーバーのリストを含む署名付きファイルへのパス。Webリソースカテゴリーのデータベースを更新するために使用されます。</p> <p>パラメータが空ではなく、指定されたファイルが存在する場合、更新にはサーバーのみが使用されます。リストのメインファイル(上記を参照)は無視されます。パラメータによって認識されたファイルが空の場合、更新の試行は失敗します。</p>



パラメータ	説明
	デフォルト値: <var_dir>/drl/dws/custom.drl <ul style="list-style-type: none">• GNU/Linuxの場合: /var/opt/drweb.com/drl/dws/custom.drl• FreeBSDの場合: /var/drweb.com/drl/dws/custom.drl
DwsDrlDir {path to directory}	標準的な更新ゾーンのサーバーに接続するためのファイルを含むディレクトリへのパスを定義します。Webリソースカテゴリーのデータベースを更新するために使用されます。 デフォルト値: <var_dir>/drl/dws <ul style="list-style-type: none">• GNU/Linuxの場合: /var/opt/drweb.com/drl/dws• FreeBSDの場合: /var/drweb.com/drl/dws
DwsCustomDrlDir {path to directory}	特別な「カスタマイズされた」更新ゾーンのサーバーに接続するためのファイルを含むディレクトリへのパスを定義します。Webリソースカテゴリーのデータベースを更新するために使用されます。 パラメータで定義されたディレクトリ内に、空でない署名付きサーバーリストファイル(.drlファイル)がある場合、更新はこれらのサーバーからのみ実行され、主要なゾーンサーバー(上記を参照)はWebリソースカテゴリーのデータベースを更新するためには使用されません。 デフォルト値: <var_dir>/custom-drl/dws <ul style="list-style-type: none">• GNU/Linuxの場合: /var/opt/drweb.com/custom-drl/dws• FreeBSDの場合: /var/drweb.com/custom-drl/dws
DwsUpdateEnabled {Boolean}	Webリソースカテゴリーのデータベースの更新が許可されているかどうかを示すインジケータ。 使用可能な値: <ul style="list-style-type: none">• Yes - 更新は許可されており、実行されます。• No - 更新は許可されていないため実行されません。 デフォルト値: Yes
AntispamDrlDir {path to directory}	パラメータは使用されません。 デフォルト値: <var_dir>/drl/antispam <ul style="list-style-type: none">• GNU/Linuxの場合: /var/opt/drweb.com/drl/antispam• FreeBSDの場合: /var/drweb.com/drl/antispam
AntispamCustomDrlDir {path to directory}	パラメータは使用されません。 デフォルト値: <var_dir>/custom-drl/antispam <ul style="list-style-type: none">• GNU/Linuxの場合: /var/opt/drweb.com/custom-drl/antispam• FreeBSDの場合: /var/drweb.com/custom-drl/antispam
AntispamUpdateEnabled {Boolean}	パラメータは使用されません。 デフォルト値: No
BackupDir {path to directory}	ロールバックに備えて、更新済みファイルの旧バージョンが保存されているディレクトリへのパス。更新するたびに、更新したファイルのみがバックアップされます。



パラメータ	説明
	デフォルト値 : /tmp/update-backup
MaxBackups <i>{integer}</i>	<p>更新済みファイルの以前のバージョンの最大保存数。この数を超えると、最も古いコピーが次の更新時に削除されます。</p> <p>パラメータ値がゼロの場合、以前のバージョンのファイルは保存されません。</p> <p>デフォルト値 : 0</p>
IdleTimeLimit <i>{time interval}</i>	<p>コンポーネントの最大アイドル時間。指定された時間が経過すると、コンポーネントはシャットダウンします。</p> <p>このコンポーネントは、スケジュールによる次の更新時または明示的なコマンド <code>drweb-ctl update [--local-cloud]</code> で起動されます。更新が完了すると、指定された時間、待機します。新しいリクエストがない場合は (UseLocalCloud = Yes の場合のクラウドとのインタラクションを含む)、次の更新を試行するまでシャットダウンします。</p> <p>指定可能な値 : 10秒 (10s) から 30日 (30d) まで。 None 値が設定されている場合、コンポーネントは永続的に機能します。コンポーネントがアイドル状態になると、SIGTERM シグナルは送信されません。</p> <p>デフォルト値 : 30s</p>
UseLocalCloud <i>{Boolean}</i>	<p>Dr.Web 更新サーバーに加えて、Dr.Web MeshD コンポーネント経由で Dr.Web for UNIX 製品のローカルクラウドと連携して、更新を同期します (クラウドに更新を送信し、クラウドから更新を取得します)。</p> <p>使用可能な値 :</p> <ul style="list-style-type: none">• No - 更新には Dr.Web 更新サーバーのみ使用します。クラウドとの更新の同期は無効ですが、<code>drweb-ctl update --local-cloud</code> コマンドを使用して明示的に実行できます。• Yes - ホスト上の更新をローカルクラウドと同期します (利用可能な更新がある場合はクラウドから更新を取得し、ホスト上の更新の方が新しい場合はクラウドに更新を送信します)。 <p>デフォルト値 : Yes</p>



Dr.Web ES Agent

アンチウイルス集中管理エージェントDr.Web ES Agentは、Dr.Web for UNIX Internet Gatewaysを[集中管理](#)サーバー(Dr.Web Enterprise Serverなど)に接続するように設計されています。

Dr.Web for UNIX Internet Gatewaysが集中管理サーバーDr.Web ES Agentに接続されている場合、ローカル設定とライセンス[キーファイル](#)は、集中管理サーバーに保存されているキーファイルに応じて同期されます。さらにDr.Web ES Agentは、ウイルスイベントに関する統計情報や実行中のコンポーネントのリストとそのステータスを集中管理サーバーに送信します。

またDr.Web ES Agentは、更新コンポーネント[Dr.Web Updater](#)を経由せずに、接続されている集中管理サーバーから直接Dr.Web for UNIX Internet Gatewaysのウイルスデータベースを更新します。

動作原理

Dr.Web ES Agentは集中管理サーバー(Dr.Web Enterprise Serverなど)への接続を確立します。これにより、ネットワーク管理者はネットワーク内で共通のセキュリティポリシーを実装し、特にすべてのネットワーク端末とサーバーに対して同じスキャン設定と脅威検出への対応を設定できます。さらに、集中管理サーバーは最新のウイルスデータベースを保存するので、ネットワークの内部更新サーバーの役割も果たします(この場合、更新はDr.Web ES Agentで実行され、[Dr.Web Updater](#)は使用されません)。

Dr.Web ES Agentを集中管理サーバーに接続する際、エージェントはプログラムコンポーネントとライセンスキーファイルの最新の設定を受信したことを確認します。その後、それらの設定は[Dr.Web ConfigD](#)設定デーモンに送信されて、管理対象のコンポーネントに適用されます。さらに、コンポーネントは端末のファイルシステムオブジェクトをスキャンするタスク(スケジュールされたタスクを含む)も受信します。

Dr.Web ES Agentは、検出された脅威と適用されたアクションに関するサーバーの統計情報を収集して送信します。

Dr.Web ES Agentを集中管理サーバーに接続するには、ホスト(集中管理サーバーでは「端末」)のパスワードとIDに加えて、認証のためにサーバーによって使用されるパブリック暗号化キーファイルが必要です。端末IDの代わりに、端末が含まれるプライマリグループのIDを指定できます。必要なIDとパブリックキーファイルについては、アンチウイルスネットワークの管理者にお問い合わせください。

さらに、このオプションが集中管理サーバーで許可されている場合は、保護されたサーバー(「ワークステーション」)にホストを「新規端末」として接続できます。この場合、管理者が接続リクエストを確認した後に、集中管理サーバーでは自動的にIDとパスワードを生成し、今後の接続のためにそれをエージェントに送信します。

コマンドライン引数

Dr.Web ES Agentを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-esagent [ <parameters> ]
```

Dr.Web ES Agentは次のオプションを処理できます。

パラメータ	説明
-------	----



<code>--help</code>	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了します。 短縮形： <code>-h</code> 引数：なし
<code>--version</code>	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了します。 短縮形： <code>-v</code> 引数：なし

例：

```
$ /opt/drweb.com/bin/drweb-esagent --help
```

このコマンドは、Dr.Web ES Agentに関する簡単なヘルプ情報を出力します。

スタートアップノート

このコンポーネントは、自律モードで(他のコンポーネントから自律的に)OSのコマンドラインから直接起動することはできません。OSの起動時にDr.Web ConfigD設定デーモンによって自動的に起動します。コンポーネントの動作を管理し、Dr.Web for UNIX Internet Gatewaysを集中管理サーバーに接続するには、Dr.Web for UNIX Internet Gateways用のコマンドラインベース管理ツールDr.Web Ctを使用できます(これはdrwebctlコマンドを使用して呼び出されます)。



コマンドラインから製品のこのコンポーネントに関するドキュメントを取得するには、`man 1 drweb-esagent`コマンドを使用します。

設定パラメータ

このコンポーネントは、Dr.Web for UNIX Internet Gatewaysの統合された設定ファイルの[ESAgent]セクションで指定されている設定パラメータを使用します。


セクションには以下のパラメータが含まれています。

パラメータ	説明
<code>LogLevel</code> <i>{logging level}</i>	コンポーネントのロギングレベル。 パラメータの値が指定されていない場合は、[Root]セクションのDefaultLogLevelパラメータの値が使用されます。 デフォルト値：Notice
<code>Log</code> <i>{log type}</i>	コンポーネントのロギング方式。 デフォルト値：Auto
<code>ExePath</code> <i>{path to file}</i>	コンポーネントの実行パス。 デフォルト値：<opt_dir>/bin/drweb-esagent



パラメータ	説明
	<ul style="list-style-type: none">• GNU/Linuxの場合 : /opt/drweb.com/bin/drweb-esagent• FreeBSDの場合 : /usr/local/libexec/drweb.com/bin/drweb-esagent
DebugIpc {Boolean}	IPCメッセージをデバッグログ <code>LogLevel = DEBUG</code> に書き込みます (Dr.Web ES AgentとDr.Web ConfigD設定デーモンとの間のやり取り)。 デフォルト値 : No
MobileMode {On / Off / Auto}	集中管理サーバーに接続したときのモバイルモードを有効 / 無効にします。 使用可能な値 : <ul style="list-style-type: none">• On - 集中管理サーバーで許可される場合は、モバイルモードを使用します (つまり、Dr.Web Updaterを介してDoctor Webの更新サーバーから更新を実行します)。• Off - モバイルモードを使用せずに、集中管理モードで動作を継続します (更新は常に集中管理サーバーから受信します)。• Auto - 集中管理サーバーで許可される場合は、モバイルモードを使用し、使用できる接続や接続品質の高さに応じて、Dr.Web Updaterを介したDoctor Webの更新サーバーと集中管理サーバーの両方から更新を実行します。 このパラメータの動作はサーバーの権限に依存することに注意してください。モバイルモードが使用するサーバーで許可されていない場合、このパラメータは無効です。 デフォルト値 : Auto
Discovery {On / Off}	エージェントが、集中管理サーバーに組み込まれているネットワークインスペクターからの <i>discovery</i> リクエストの受信を有効にするかどうかを指定します (<i>discovery</i> リクエストは、アンチウイルスネットワークの構造と状態を確認するためにインスペクターによって使用されます)。 使用可能な値 : <ul style="list-style-type: none">• On - <i>discovery</i> リクエストの受信と処理を有効にします。• Off - <i>discovery</i> リクエストの受信と処理を無効にします。 このパラメータは集中管理サーバーの設定よりも優先順位が高いことに注意してください。パラメータ値が <code>Off</code> に設定されている場合、このオプションがサーバーで有効になっていても、エージェントは <i>discovery</i> リクエストを受信しません。 デフォルト値 : On
UpdatePlatform {platform name}	エージェントが、集中管理サーバーからのスキャンエンジンの更新の受信を有効にするかどうかを指定します。スキャンエンジンは指定のプラットフォーム向けに開発されています。プラットフォーム名は、プラットフォーム名を含む文字列です。 使用可能な値 : <ul style="list-style-type: none">• GNU/Linuxの場合 : <code>unix-linux-32</code>、<code>unix-linux-64</code>、<code>unix-linux-mips</code>• FreeBSDの場合 : <code>unix-freebsd-32</code>、<code>unix-freebsd-64</code>• Darwinの場合 : <code>unix-darwin-32</code>、<code>unix-darwin-64</code>



パラメータ	説明
	<div data-bbox="576 255 1450 383" style="background-color: #fff9c4; padding: 10px;"> パラメータ値は確実に変更が必要な場合にのみ変更することを強くお勧めします。</div> <p data-bbox="539 405 1171 439">デフォルト値: 現在使用されているプラットフォームによる</p>
SrvMsgAutoremove <i>{integer}</i>	<p data-bbox="539 461 1390 495">集中管理サーバーからのメッセージが自動的に削除されるまでの保存期間</p> <p data-bbox="539 524 1347 591">使用可能な値: 1週間 (1w) から365日 (365d) まで 保存期間は整数で、サフィックス (s、m、h、d、w) を付けて指定します。</p> <p data-bbox="539 622 727 656">デフォルト値: 1w</p>



Dr.Web HTTPD

Dr.Web HTTPDは、HTTP経由で(たとえばWebブラウザ経由で) Dr.Web for UNIX Internet Gatewaysとローカルおよびリモートで対話するためのインフラストラクチャを提供します。このコンポーネントは、Dr.Web for UNIX Internet Gatewaysを管理するためのインターフェースを提供します。

Dr.WebのWebインターフェースを介してDr.Web for UNIX Internet Gatewaysを管理するだけでなく、Dr.Web HTTPDのコマンドインターフェース(HTTP API)を直接使用し、HTTPSを介してDr.Web for UNIX Internet Gatewaysのコンポーネントと対話することもできます。この機能により、Dr.Web for UNIX Internet Gatewaysを管理するための独自のインターフェースを作成できます。

Dr.Web HTTPDが提供するHTTP APIの詳細については、[該当するセクション](#)を参照してください。

安全なHTTPS接続を使用するには、適切なSSLサーバー証明書とプライベートキーをDr.Web HTTPDに提供する必要があります。デフォルトでは、インストール中にDr.Web HTTPD用のSSLサーバー証明書とSSLプライベートキーが自動的に生成されますが、必要に応じて独自の証明書とキーを生成することもできます。また、Dr.Web HTTPDによって信頼されている認証局証明書で署名されたユーザーの個人用認証証明書を、Dr.Web HTTPDに接続するときの自動クライアント認証に使用することもできます。

SSLキーと証明書を生成するには、`openssl`ユーティリティを使用できます。`openssl`ユーティリティを使用して証明書とプライベートキーを生成する方法の例については、[付録E. SSL証明書を生成する](#)のセクションを参照してください。

動作原理

Dr.Web HTTPDはDr.Web for UNIX Internet Gatewaysの動作を管理するためのWebサーバーです。Dr.Web HTTPDがあれば、外部Webサーバー(Apache HTTP ServerやNginxなど)やWebminなどの管理サービスを使用せずに済みます。さらにこのコンポーネントは、同じホスト上にあるそのようなサーバーやサービスと同時に機能することができ、それらの動作を妨げることはありません。

Dr.Web HTTPDサーバーは、HTTPおよびHTTPSプロトコルを介し、設定で指定されたソケットで受信したリクエストを処理します。このため、このサーバーは、Webサーバーと同じホスト上で動作しているときに、それらのサーバーと競合することはありません。Dr.Web for UNIX Internet Gatewaysの管理には、安全なHTTPSプロトコルが使用されます。



Dr.Web管理Webインターフェースをインストールすることは、Dr.Web for UNIX Internet Gatewaysを正しく機能させるための必須事項ではありません。インストールしなくても問題ありません。対応するブロックが破線で囲まれているのはこのためです。

Dr.Web HTTPDコンポーネントは、Dr.Web for UNIX Internet Gateways [Dr.Web ConfigD](#)設定デーモンの他、ファイルスキャン用の[Dr.Web File Checker](#)コンポーネントやその他のコンポーネントにコマンドを送信します。これらのコマンドは、提供されているHTTP APIを介して受信したコマンドに基づいています。

Dr.Web HTTPDを使用するDr.Web for UNIX Internet Gatewaysの管理WebインターフェースがDr.Web for UNIX Internet Gatewaysに含まれている場合は、該当する[セクション](#)にその説明が記載されています。

Dr.Webの管理WebインターフェースがDr.Web for UNIX Internet Gatewaysに含まれていない場合は、Dr.Web HTTPDによるHTTP APIを対話に使用する、任意の外部管理インターフェースを接続できます([HTTP APIの説明](#)のセクションで説明しています)。



コマンドライン引数

Dr.Web HTTPDを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-httpd [<options>]
```

Dr.Web HTTPDは次のオプションを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了します。 短縮形：-h 引数：なし
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了します。 短縮形：-v 引数：なし

例：

```
$ /opt/drweb.com/bin/drweb-httpd --help
```

このコマンドは、Dr.Web HTTPDに関する簡単なヘルプ情報を出力します。

スタートアップノート

このコンポーネントは、自律モードで(他のコンポーネントから自律的に)OSのコマンドラインから直接起動することはできません。必要に応じて[Dr.Web ConfigD](#)設定デーモンによって自動的に起動されます(通常はOSの起動時)。コンポーネントが実行されていて、Webインターフェースがインストールされている場合は、標準のWebブラウザを使用して、Webインターフェースが提供されているアドレスにHTTPS経由でアクセスするだけで、Dr.Web for UNIX Internet Gatewaysのコンポーネントを管理できます。コンポーネントの動作を管理するには、Dr.Web for UNIX Internet Gateways用のコマンドラインベース管理ツール[Dr.Web Ct](#)を使用できます(これはdrweb-ctl1[コマンド](#)を使用して呼び出されます)。



コマンドラインから製品のこのコンポーネントに関するドキュメントを取得するには、`man 1 drweb-httpd`コマンドを使用します。

設定パラメータ

このコンポーネントは、Dr.Web for UNIX Internet Gatewaysの統合された[設定ファイル](#)の[HTTPD]セクションで指定されている設定パラメータを使用します。



セクションには以下のパラメータが含まれています。

パラメータ	説明
LogLevel <i>{logging level}</i>	コンポーネントの ロギングレベル 。 パラメータの値が指定されていない場合は、[Root] セクション の DefaultLogLevelパラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行パス。 デフォルト値: <opt_dir>/bin/drweb-httpd <ul style="list-style-type: none">GNU/Linuxの場合: /opt/drweb.com/bin/drweb-httpdFreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-httpd
Start <i>{Boolean}</i>	Dr.Web ConfigD 設定デーモンによってコンポーネントを起動するかどうかを指定します。 このパラメータに Yes値を指定すると、設定デーモンはただちにコンポーネントを開始します。また、No値を指定すると、設定デーモンはただちにコンポーネントを終了します。 デフォルト値: 管理インターフェースがインストールされているかどうかによって異なります。
AdminListen <i>{address, ...}</i>	Dr.Web HTTPDが、管理者権限を持つクライアントからの (HTTPS経由での) 接続をリッスン (待ち受け) しているネットワークソケット (すべてのネットワークソケットは <IP address>:<port>で構成されます) のリスト。これらのソケットは、管理 Webインターフェース (Webインターフェースがインストールされている場合) への接続とHTTP APIへのアクセスの両方に使用されます。 リストの値は、コンマ (引用符内の各値) で区切る必要があります。パラメータはセクションで複数回指定できます (この場合、そのすべての値が1つのリストにまとめられます)。 例: ソケット 192.168.0.1:1234および10.20.30.45:5678をリストに追加します。 <ol style="list-style-type: none">設定ファイルに値を追加します。<ul style="list-style-type: none">1行に2つの値: <pre>[HTTPD] AdminListen = "192.168.0.1:1234", "10.20.30.45:5678"</pre>2行 (1行に1つの値): <pre>[HTTPD] AdminListen = 192.168.0.1:1234 AdminListen = 10.20.30.45:5678</pre>



パラメータ	説明
	<p>2. drweb-ctl cfset コマンドを使用して値を追加します。</p> <pre data-bbox="619 293 1437 465"># drweb-ctl cfset HTTPD.AdminListen -a 192.168.0.1:1234 # drweb-ctl cfset HTTPD.AdminListen -a 10.20.30.45:5678</pre> <p>値が指定されていない場合、HTTP APIとWebインターフェース(インストールされている場合)を使用することはできません。</p> <p>デフォルト値: 127.0.0.1:4443</p>
PublicListen {address, ...}	<p>Dr.Web HTTPDが、制限された権限を持つクライアントからの(HTTP経由での)接続をリッスン(待ち受け)しているネットワークソケット(すべてのネットワークソケットは <IP address>:<port>で構成されます)のリスト</p> <p>リストの値は、コンマ(引用符内の各値)で区切る必要があります。パラメータはセクションで複数回指定できます(この場合、そのすべての値が1つのリストにまとめられます)。</p> <p>例: ソケット192.168.0.1:1234および10.20.30.45:5678をリストに追加します。</p> <ol style="list-style-type: none">設定ファイルに値を追加します。<ul style="list-style-type: none">1行に2つの値:<pre data-bbox="619 1025 1437 1167">[HTTPD] PublicListen = "192.168.0.1:1234", "10.20.30.45:5678"</pre>2行(1行に1つの値):<pre data-bbox="619 1223 1437 1364">[HTTPD] PublicListen = 192.168.0.1:1234 PublicListen = 10.20.30.45:5678</pre>drweb-ctl cfset コマンドを使用して値を追加します。<pre data-bbox="619 1442 1437 1608"># drweb-ctl cfset HTTPD.PublicListen -a 192.168.0.1:1234 # drweb-ctl cfset HTTPD.PublicListen -a 10.20.30.45:5678</pre> <p>これらのアドレス(ソケット)では、HTTP APIのすべてのコマンドにアクセスしたり、管理Webインターフェースにアクセスしたりすることはできません。</p> <p>デフォルト値: (未設定)</p>
AdminSslCertificate {path to file}	<p>Webインターフェースサーバーが管理ソケットへの接続を確立するクライアントとHTTPS経由で通信するために使用するサーバー証明書ファイルへのパス。</p> <p>このファイルは、コンポーネントのインストール中に自動的に生成されます。</p> <p>証明書ファイルとプライベートキーファイル(後述のパラメータで指定されます)は、一致するペアを形成する必要があります。</p>



パラメータ	説明
	<p>デフォルト値: <code><etc_dir>/certs/serv.crt</code></p> <ul style="list-style-type: none">GNU/Linuxの場合: <code>/etc/opt/drweb.com/certs/serv.crt</code>FreeBSDの場合: <code>/usr/local/etc/drweb.com/certs/serv.crt</code>
AdminSslKey <i>{path to file}</i>	<p>Webインターフェースサーバーが管理ソケットへの接続を確立するクライアントとHTTPS経由で通信するために使用するプライベートキーファイルへのパス。</p> <p>このファイルは、コンポーネントのインストール中に自動的に生成されます。</p> <p>証明書ファイル(前述のパラメータで指定されます)とプライベートキーファイルは、一致するペアを形成する必要があります。</p> <p>デフォルト値: <code><etc_dir>/certs/serv.key</code></p> <ul style="list-style-type: none">GNU/Linuxの場合: <code>/etc/opt/drweb.com/certs/serv.key</code>FreeBSDの場合: <code>/usr/local/etc/drweb.com/certs/serv.key</code>
AdminSslCA <i>{path to file}</i>	<p>HTTPS経由で管理ソケットに接続しているクライアントから提供された証明書をチェックするための、信頼できる認証局(CA)の証明書として機能する証明書ファイルへのパス</p> <p>クライアントの証明書が、このパラメータで指定された証明書で署名されている場合、このクライアントは認証のためにログイン情報/パスワードのペアを入力する必要はありません。また、このパラメータで設定された証明書で署名されているクライアント証明書を使用するクライアントでは、ログイン情報/パスワードによる認証は禁止されます。</p> <p>この証明書ベースの認証に成功したクライアントは、常にスーパーユーザー(<code>root</code>)として扱われます。</p> <p>デフォルト値: (未設定)</p>
WebconsoleRoot <i>{path to directory}</i>	<p>管理Webインターフェースがインストールされている場合に、その管理Webインターフェースによって使用されるファイルがあるディレクトリ(Apache HTTP Serverの<code>htdocs</code>ディレクトリ相当)へのパス</p> <p>デフォルト値: <code><opt_dir>/share/drweb-httpd/webconsole</code></p> <ul style="list-style-type: none">GNU/Linuxの場合: <code>/opt/drweb.com/share/drweb-httpd/webconsole</code>FreeBSDの場合: <code>/usr/local/libexec/drweb.com/bin/drweb-httpd/webconsole</code>
AccessLogPath <i>{path to file}</i>	<p>クライアントからWebインターフェースサーバーへのすべてのHTTP/HTTPSリクエストが登録されるファイルへのパス。</p> <p>指定しない場合、HTTP/HTTPSリクエストはファイルに記録されません。</p> <p>デフォルト値: (未設定)</p>

HTTP APIの説明

このセクションの内容

- 概要



- [ユーザー認証と承認](#)
- [Dr.Web for UNIX Internet Gatewaysの管理](#)
- [脅威のリストの管理](#)
- [隔離の管理](#)
- [HTTP APIの使用例](#)

1. 概要

HTTP APIは、HTTPプロトコルを介してDr.Web for UNIX Internet Gatewaysを制御および管理する手段として提供されます（セキュリティを確保するために、HTTPSプロトコルが使用されます）。

HTTPプロトコルのバージョン1.0が使用されます。APIは、HTTPプロトコルの標準メソッドであるGETとPOSTを使用します。特に指定がない限り、すべてのデータはJSONオブジェクトの形式で送信されます。HTTP POSTリクエストの本文でJSONオブジェクトを送信する場合は、Content-Type:ヘッダーをapplication/jsonの値で使用します。

HTTPリクエストに対するHTTPレスポンスのフォーマット

- 特に指定のない限り、すべてのリクエストへのレスポンスとしてJSONオブジェクトが返されます。リクエストの処理中にエラーが発生した場合、[Error](#) JSONが返されます。
- レスポンスとして送信されたJSONオブジェクトにArrayタイプのフィールドがあり、この配列に要素が1つも含まれていない場合、このフィールドはサーバーからのレスポンスから省略されます。
- 特に指定のない限り、すべてのレスポンスのContent-Type:ヘッダーフィールドにはapplication/json値があります。
- 存在しないエンドポイントをクライアントが要求した場合、コードフィールドにEC_UNEXPECTED_MESSAGEが含まれる[Error](#) JSONオブジェクトが返されます。
- SCS (*Secure Cookie Sessions for HTTP*) が使用されている場合 ([以下](#)を参照)、レスポンスにはSCS *cookie*が含まれます。

JSONオブジェクト内の文字列のエンコード

- 文字列はUTF-8エンコーディング (BOMなし) で送信されます。ASCII表の一部ではない記号は、送信JSON文字列内で\uXXXXのようなシーケンスでエスケープされませんが、UTF-8エンコードで送信されます。
- 受信JSONオブジェクトの文字列には、UTF-8でエンコードされた記号と\uXXXXのようなエスケープシーケンスの両方を含めることができます。

データ転送に関する一般的な制限

- 本文にJSONオブジェクトが含まれるPOSTリクエストでは、[RFC 7159](#)に準拠するすべての記号が許可されます。
- GETリクエストでは、[RFC 1945](#)に準拠するすべての記号がURIで許可されます。
- [RFC 1945](#)に準拠する記号は、リクエストの他のどの部分 (ヘッダーまたは本文) でも使用できます。



2. ユーザー認証と承認

APIの使用を開始するには、サーバーによる認証が必要です。承認の手段は2つ用意されています。

1. [RFC 6896](#)に準拠したSCSを使用する。
2. Dr.Web HTTPDが信頼できるCAの証明書と見なす特別な証明書で署名された、[クライアントのSSL証明書を使用する](#)。この場合、クライアントは、認証を受けるためにルートの認証情報を正しく入力したかのように扱われます(X.509クライアント証明書が使用されます)。

SCSを使用する場合、認証を確認するcookieは、リクエストではCookie:、レスポンスではSet-Cookie:がヘッダーで送信されます。

SSL証明書による承認の場合、cookieは使用されません。

SCSで承認する場合、loginコマンドを送信することでAPIの使用が始まります。このコマンドが正常に実行されると、レスポンスとしてSCS cookieがクライアントに送信されます。

クライアント証明書で承認する場合、loginコマンドを実行する必要はありません。実行しようとすると、レスポンスにError JSONオブジェクトが返されます。

2.1. ログインとパスワードを指定する(SCS)

ユーザー認証および承認コマンド:

APIコマンド	説明
login	<p>アクション: 指定されたユーザー名とパスワードに基づいてクライアントを認証し、HTTP APIのコマンドを使用することをクライアントに許可します。認証が成功すると、SCS cookieが返されます。</p> <p>URI: /api/10.2/login</p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: AuthOptionsオブジェクト</p> <p>正常に実行された結果: 空のオブジェクト、SCS cookie</p>
logout	<p>アクション: 提供されたSCS cookieを取り消します。その後、取り消されたSCS cookieを含むHTTP API呼び出しへのレスポンスとして、EC_NOT_AUTHORIZEDエラーコードを含むErrorオブジェクトが返されます。</p> <p>URI: /api/10.2/logout</p> <p>HTTPメソッド: GET</p> <p>入力パラメータ: SCS cookie</p> <p>正常に実行された結果: 空のオブジェクト</p>
whoami	<p>アクション: 認証されたユーザーの名前を表示します。</p> <p>URI: /api/10.2/whoami</p> <p>HTTPメソッド: GET</p>



APIコマンド	説明
	入力パラメータ: (SCS cookie)* 正常に実行された結果: whoami オブジェクト、(SCS cookie)

*) SCS cookieは、SCSによる認証が使用される場合にのみ送受信する必要があるため、これ以降は括弧に入れて表記します。



SCSで認証する場合にのみ、loginとlogoutコマンドが使用されます。

使用されるオブジェクトの説明

1) AuthOptions - 完全なHTTP APIを使用するために認証および承認される必要があるユーザーのログインデータを含むオブジェクト:

```
{
  "user": string, //User name
  "password": string //User's password
}
```



管理者グループ (DebianとUbuntuでは `sudoers`、CentOSとFedoraでは `wheel`、Astra Linuxでは `astra-admin` など) のメンバーであるユーザーを指定できます。ユーザーが管理者グループのメンバーでない場合、レスポンスに `EC_NOT_AUTHORIZED` エラーが返されます。

2) whoami - HTTP APIを使用することを許可されたユーザーの名前を含むオブジェクト:

```
{
  "whoami" :
  {
    "user": string //User name
  }
}
```

3) Error - 発生したエラーに関する情報を含むオブジェクト:

```
{
  "error" :
  {
    "code" : string, //A string specifying an error code that looks like
    EC_XXX
    *"what": string //Description of the error
  }
}
```

アスタリスク(*)のパラメータは任意です。



リクエストの処理中にエラーが発生した場合にHTTP APIコマンドへのレスポンスとして返される **Error** JSONオブジェクトには、数値のエラーコードではなく、Dr.Web for UNIX Internet Gatewaysのコンポーネントによって使用される内部文字列型コードを含むcodeフィールドがあります。このコードは、EC_XXXのような文字列です。対応する数値コードやエラーの詳細情報を確認するには、『管理者マニュアル』の付録Fにある「[既知のエラー](#)」セクションを参照してください。

2.2. 個人証明書を使用する認証

SSL証明書による認証は、Dr.Web HTTPDの設定で信頼済みとして指定された認証局証明書によって個人証明書が署名されていることを前提としています。証明書で認証された場合、すべてのリクエストはrootユーザーの権限で行われたものと見なされます。

個人ユーザー証明書で承認するには

1. 認証局証明書で署名された個人証明書を作成します。
2. Dr.Web HTTPDの[設定](#) (パラメータAdminSslCA)で、個人証明書に署名する認証局証明書へのパスを指定します。
3. Dr.Web HTTPDに接続するたびに、署名付き証明書を使用します。

必要に応じて、[付録E. SSL証明書を生成する](#)のセクションを参照してください。

3. Dr.Web for UNIX Internet Gatewaysを管理する

設定パラメータの現在の値を表示および変更するためのAPIコマンド:

APIコマンド	説明
設定を管理するコマンド	
get_lexmap	<p>アクション: 現在の設定 (ここではパラメータの「語彙マップ」と呼ばれます)のパラメータ値を取得します。</p> <p>URI: /api/10.2/get_lexmap</p> <p>HTTPメソッド: GET</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: LexMapsオブジェクト、(SCS cookie)</p>
set_lexmap	<p>アクション: 現在の設定の指定されたパラメータを設定または(デフォルトに)リセットします (パラメータの「語彙マップ」として送信されます)。</p> <p>URI: /api/10.2/set_lexmap</p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (SCS cookie)、LexMapオブジェクト</p> <p>正常に実行された結果: SetOptionResultオブジェクト、(SCS cookie)</p>



APIコマンド	説明
コマンドの更新	
start_update	<p>アクション: 更新を起動します。</p> <p>URI: /api/10.2/start_update</p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: StartUpdateオブジェクト、(SCS cookie)</p>
stop_update	<p>アクション: アクティブな更新プロセスを停止します。</p> <p>URI: /api/10.2/stop_update</p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: 空のオブジェクト、(SCS cookie)</p>
baseinfo	<p>アクション: ダウンロードしたウイルスベースに関する情報を表示します。</p> <p>URI: /api/10.2/baseinfo</p> <p>HTTPメソッド: GET</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: VirusBaseInfoオブジェクトを含むBaseInfoResultオブジェクト (SCS cookie)</p>
ライセンス管理コマンド	
install_license	<p>アクション: 指定されたキーファイルをインストールします。</p> <p>URI: /api/10.2/install_license</p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (SCS cookie)、キーファイル本体 (またはキーファイルを含むアーカイブ)</p> <p>正常に実行された結果: 空のオブジェクト、(SCS cookie)</p>
集中管理サーバーに接続するためのコマンド	
esconnect	<p>アクション: 集中管理モードを有効にします。</p> <p>URI: /api/10.2/esconnect</p> <p>HTTPメソッド: POST</p>



APIコマンド	説明
	入力パラメータ: (SCS cookie)、 ESConnection オブジェクト 正常に実行された結果: 空のオブジェクト、(SCS cookie)
esdisconnect	アクション: 集中管理モードを無効にします。 URI: /api/10.2/esdisconnect HTTPメソッド: POST 入力パラメータ: (SCS cookie) 正常に実行された結果: 空のオブジェクト、(SCS cookie)

製品のコンポーネントの設定が返され、いわゆる語彙マップ、つまり一連のパラメータと値のペアとして設定されません。[LexMaps](#)オブジェクトには常に3つの[LexMaps](#)オブジェクトが含まれます。

- *active* - パラメータの現在の値
- *hardcoded* - 値がない、または無効な値のパラメータに自動的に割り当てられるデフォルト値
- *master* - クライアントによって設定された設定パラメータの値



`get_lexmap`コマンドは、実際にインストールされて実行されているコンポーネントだけでなく、Dr.Web for UNIX Internet Gatewaysに含めることができるすべてのコンポーネントについて、常に3つすべての設定パラメータ値を返します。

JSONオブジェクトの説明

1) `LexMaps` - パラメータ値のアクティブ、デフォルト、およびユーザー設定の語彙マップを含むオブジェクト。

```
{
  "active": LexMap, //Active (current) values of configuration parameters
  "hardcoded": LexMap, //Default values of configuration parameters
  "master": LexMap //Configuration parameter values set
  //by the user
}
```

これらの各フィールドは、次に[LexOption](#)オブジェクトの配列が格納される[LexMap](#)オブジェクトです。

2) `LexMap` - パラメータの語彙マップを含むオブジェクト。

```
{
  "option": LexOption[] //Array of configuration options
}
```

3) `LexOption` - 単一のパラメータまたは設定のセクション(パラメータのグループ)を含むオブジェクト。

```
{
  "key": string, //Name of the option (configuration parameter/section)
  *"value": LexValue, //If this option is a single parameter
  *"map": LexMap //If this option is a section
}
```



アスタリスク(*)のパラメータは任意です。

LexOptionオブジェクトは、Dr.Web for UNIX Internet Gatewaysの設定のセクションまたは単一のパラメータを表します。このオブジェクトには、常にセクションの名前または単一のパラメータの名前に対応するkeyフィールドがあります。これに加えて、このオブジェクトが表すもの(単一のパラメータまたはセクション)に応じて、valueフィールド(単一のパラメータを表す場合)またはmapフィールド(セクションを表す場合)もあります。セクションもまた、**LexMap**タイプのオブジェクトです。一方、単一のパラメータの値は、パラメータの値を文字列形式で指定するitemフィールドを含む**LexValue**タイプのオブジェクトです。

- 4) LexValue - パラメータに割り当てられた値の配列を含むオブジェクト。

```
{
  "item": string[] //Array of parameter values
}
```

set_lexmapコマンドは、その入力として**LexMap**オブジェクトを受け取ります。これには、値を新しい値に変更するか、デフォルトにリセットするすべてのパラメータを含める必要があります。デフォルト値にリセットするパラメータには、valueフィールドを含めないでください。ユーザーがset_lexmapコマンドで指定した語彙マップに記載されていないパラメータは変更されません。set_lexmapコマンドは、その実行の結果として、コマンドで指定されたすべてのパラメータの変更結果を含む**SetOptionResult**オブジェクトを返します。

- 5) SetOptionResult - itemフィールドにパラメータの変更結果の配列を含むオブジェクト。

```
{
  "item": SetOptionResultItem[] //Array of results
}
```

このオブジェクトには、コマンドで指定されたすべてのパラメータの変更結果を表す**SetOptionResultItem**オブジェクトの配列が含まれています。

- 6) SetOptionResultItem - あるパラメータの値を変更することに関する情報を含むオブジェクト。

```
{
  "option": string, //Name of the parameter
  "result": string, //Result of changing the value (error code)
  *"lower_limit": string, //The lowest permitted value
  *"upper_limit": string //The highest permitted value
}
```

アスタリスク(*)のパラメータは任意です。

optionフィールドには、アクションが適用されたパラメータの名前が含まれており、resultフィールドには、このパラメータの値を変更しようとした結果が含まれています。新しい値がパラメータに正常に割り当てられた場合、このフィールドにはEC_OKが含まれます。エラーの場合(このフィールドがEC_OKに等しくない場合)、このオブジェクトには、このパラメータの最大許容値と最小許容値を保持するlower_limitフィールドとupper_limitフィールドをオプションで含めることができます。

- 7) StartUpdateオブジェクトには、開始された更新プロセスに関するデータが含まれます。

```
{
  "start_update":
  {
    "attempt_id" : number //Identifier of a launched updating process
  }
}
```

- 8) ESConnectionオブジェクトには、開始された更新プロセスに関するデータが含まれます。



```
{
  *"server": string,    //<Host address>:<port> (without the http/https
prefix)
  "certificate": string, //Base64 server key
  *"newbie": boolean,   //False by default
  *"login": string,     //User name
  *"password": string   //Password
}
```

アスタリスク(*)のパラメータは任意です。

パラメータloginとpasswordは、newbie = trueの場合にのみ指定されます。
接続前に、集中管理サーバーから証明書ファイルをダウンロードし、次のコマンドを実行します。

```
$ cat certificate.pem |base64
```

このコマンドを実行して得られた文字列がcertificateのパラメータ値として使用されます。

9) BaseInfoResultオブジェクトには、ダウンロードしたウイルスベースのデータが含まれます。

```
{
  "vdb_base_stamp" : number //Timestamp of the base
  "vdb_bases" : VirusBaseInfo[] //Detailed information upon the base
}
```

10) VirusBaseInfoオブジェクトには、各ウイルスベースに関する情報が含まれます。

```
{
  "path" : string //Path to the base file
  "virus_records" : number //The number of records in the base
  "version" : number //Base version
  "timestamp" : number //Base timestamp
  "md5" : string //base MD5-hash
  "load_result" : string //The result of downloading the base (EC_OK if
the base has been downloaded successfully)
  *"sha1" : string - base SHA1-hash
}
```

アスタリスク(*)のパラメータは任意です。

4. オブジェクトのスキャン

オブジェクトをスキャンするためのAPIコマンド:

APIコマンド	説明
データスキャン (Dr.Web Network Checkerコンポーネント呼び出しを使用)	
scan_request	アクション: 必要なパラメータを使用してデータをスキャンする接続 (endpoint) の順序。 URI: /api/10.2/scan_request HTTPメソッド: POST



APIコマンド	説明
	入力パラメータ: (SCS cookie)、 ScanOptions オブジェクト 正常に実行された結果: ScanEndpoint オブジェクト、(SCS cookie)
scan_endpoint	アクション: 作成された <i>endpoint</i> 接続でのデータスキャン(ファイル本体など)の起動。 URI: /api/10.2/scan_endpoint/ <endpoint> HTTPメソッド : POST 入力パラメータ: (SCS cookie)、検証可能なデータ 正常に実行された結果: ScanResult オブジェクト、(SCS cookie)
scan_path	アクション: 指定されたパスにあるファイルまたはディレクトリをスキャンします。 URI: /api/10.2/scan_path HTTPメソッド : POST 入力パラメータ: (SCS cookie)、 ScanPathOptions オブジェクト 正常に実行された結果: ScanPathResult オブジェクト、(SCS cookie)
scan_stat	アクション: スキャン統計の表示。 URI: /api/10.2/scan_stat HTTPメソッド : GET 入力パラメータ: (SCS cookie)、統計のフォーマット(JSONまたはCSV) 正常に実行された結果: ScanStat オブジェクト(JSON形式が選択されている場合)、(SCS cookie) CSV形式が選択されている場合、 ScanStat のフィールドに対応するテーブルが返されます。

JSONオブジェクトの説明

1) [ScanOptions](#)は、ファイルスキャン用の *エンドポイント* を作成するために使用されるパラメータを含むオブジェクトです。

```
{
  "scan_timeout_ms": number, //A time-out to scan one file, in ms
  "cure": boolean, //Apply cure to infected file
  "heuristic_analysis": boolean, //Use heuristic analysis
  "packer_max_level": number, //Maximum nesting level for packed objects
  "archive_max_level": number, //Maximum nesting level for archives
  "mail_max_level": number, //Maximum nesting level for email messaged
  "container_max_level": number, //Maximum nesting level for other
  compound objects (containers)
```



```
"max_compression_ratio": number, //Maximum a compression value
"min_size_to_scan" : number, //Minimal size of an object to be scanned
"max_size_to_scan" : number, //Maximum size of an object to be scanned
"threat_hash" : boolean //Return SHA1 and SHA256 of all threats
}
```

2) ScanPathOptionsは、指定されたパスにあるファイルまたはディレクトリをスキャンするために使用されるパラメータを含むオブジェクトです。

```
{
"path" : string //Absolute path to the file or the directory to be
scanned
*"exclude_path" : string[] //List of the paths excluded from scanning
(it is allowed to use masks)
*"scan_timeout_ms" : number //Scan timeout for an object
*"archive_max_level" : number//Maximum nesting level for archived
objects
*"packer_max_level" : number //Maximum nesting level for packed
objects
*"mail_max_level" : number //Maximum nesting level for email messages
*"container_max_level" : number//Maximum nesting level for other
compound objects (containers)
*"max_compression_ratio" : number//Maximum compression value
*"heuristic_analysis" : bool //Use heuristic analysis (true by
default)
*"follow_symlinks" : bool //Follow symbolic links
*"min_size_to_scan" : number //Minimal size of an object to be
scanned
*"max_size_to_scan" : number //Maximal size of an object to be
scanned
*"timeout_ms" : number - //Scan timeout for all objects
*"threat_hash" : bool - //Return SHA1 and SHA256 of all threats
}
```

アスタリスク(*)のパラメータは任意です。

3) ScanPathResultは、指定されたパスにあるオブジェクトのスキャン結果を含むオブジェクトです。

```
{
ScanPathResult:
"results": ScanResult[] //Scan results
*"error": string //Error if the scanning process terminated (the
scanning timeout is expired, for instance)
}
```

アスタリスク(*)のパラメータは任意です。

スキャンが成功した場合、レスポンスにはerror文字列は含まれません。

4) ScanResultは、スキャンの結果を含むオブジェクトです。

```
{
ScanResult:
"scan_report" : ScanReport //The information upon the threat found
*"sha1" : string //The SHA1 hash of the threat
}
```



```
    *"sha256" : string //The SHA256 hash of the threat
  }
```

アスタリスク(*)のパラメータは任意です。

5) ScanReportは、脅威が検出されたファイルに関する情報を含むオブジェクトです。

```
{
  ScanReport:
  "object" : string //Name of the object scanned
    For a file //The absolute path, for a nested object - the name of
the file
    Always points to temporary file when calling scan_endpoint
  *"size" : number //Object size
  *"compressed_size" : number //Object size before extraction
  *"core_fingerprint" : string //Scan engine fingerprint
  *"packer" : string[] //The list of packers used to pack the object
  *"compression_ratio" : number //Archive compression ratio
  *"archive" : Archive //Information on the archive or container type, if
the object scanned was identified as an archive or a container
  *"virus" : Virus[] //Viruses detected in the objects (if found)
  *"item" : ScanReport[] //Reports on scanning of the nested objects (if
there were some)
  *"error" : string //Scanning error (if occurred)
  *"heuristic_analysis" : bool //Indicates if heuristic analysis was used
  *"cured" : bool //The object was cured
  *"cured_by_deletion" : bool //The object was deleted.
  *"new_path" : string //The new path to the object renamed when being
cured
  *"user_time" : number //Type spent for syscalls when scanning
  *"system_time" : number //Time spent in the userspace
}
```

アスタリスク(*)のパラメータは任意です。

virusフィールドとerrorフィールドは、スキャン中に脅威が検出されず、エラーが発生しなかった場合には、存在しない可能性があります。scan_endpointを呼び出すためには、Dr.Web Network Checkerコンポーネントによってローカルサーバーファイルシステムに作成され、スキャンに関するデータを含み、scan_endpointリクエストの本文で送信される一時ファイルをscan_endpointフィールドで必ず指定します。

6) ScanEndpointは、ファイルスキャン用に作成されたエンドポイントに関するデータを含むオブジェクトです。

```
{
  "endpoint": string //Unique identifier of the created endpoint
}
```

オブジェクト本体で返されるendpoint文字列は、scan_endpointコマンド(URIの一部)でファイルスキャンを開始するために使用されます。

7) VirusInfoは、検出された脅威に関する情報を含むオブジェクトです。

```
{
  "type": string, //Type of the detected threat
  "name": string //Name of the threat
}
```



typeフィールド(脅威タイプ)は文字列SE_XXXです。

- SE_KNOWN_VIRUSは既知のウイルスです。
- SE_VIRUS_MODIFICATIONは既知のマルウェアの亜種です。
- SE_UNKNOWN_VIRUSは未知のウイルス(疑わしいオブジェクト)です。
- SE_ADWAREはアドウェアです。
- SE_DIALERはダイアラープログラムです。
- SE_JOKEはジョークプログラムです。
- SE_RISKWAREは潜在的に危険なプログラムです。
- SE_HACKTOOLはハッキングツールです。

8) Archiveは、アーカイブ、圧縮されたオブジェクト、メールメッセージ、およびその他のコンテナに関する情報を含むオブジェクトです。

```
{
  "type" : string - the type of the archive:
    "SE_ARCHIVE" - archive
    "SE_MAIL" - e-mail message
    "SE_CONTAINER" - other container
  "name" : string - archive format
}
```

9) ScanStatは、スキャン統計を含むオブジェクトです。

```
{
  "origin": string //The application by the request of which the scanning
was initialized
  #Counters for infected objects:
  "known_virus": number //Number of objects infected by known viruses
  "virus_modification": number //Number of objects infected by
modifications of known viruses
  "unknown_virus": number //Number of objects infected by unknown
viruses
  "adware": number //Number of objects with SE_ADWARE
  "dialer": number //Number of objects with SE_DIALER
  "joke": number //Number of objects with SE_JOKE
  "riskware": number //Number of objects with SE_RISKWARE
  "hacktool" : number //Number of objects with SE_HACKTOOL
  "cured": number //Number of cured threats
  "quarantined": number //Number of quarantined threats
  "deleted": number //Number of deleted threats
}
```

5. 脅威のリストの管理

スキャン中またはファイルシステムモニター(SpIDer Guard)によって検出された脅威のリストを管理できるように、HTTP APIには次のコマンドが用意されています。

APIコマンド	説明
threats	アクション: 検出されたすべての脅威のIDを一覧表示します。



APIコマンド	説明
	URI: /api/10.2/threats/ HTTPメソッド : GET 入力パラメータ: (SCS cookie) 正常に実行された結果: 脅威IDの配列
threat_info	アクション: 脅威に関する情報を脅威のIDである <threat ID>で取得します。 URI: /api/10.2/threat_info/ <threat ID> HTTPメソッド : GET 入力パラメータ: (SCS cookie) 正常に実行された結果: (SCS cookie)、 FileThreat オブジェクト
cure_threat	アクション: 脅威のIDである <threat ID>で指定された脅威の修復を試みます。 URI: /api/10.2/cure_threat/ <threat ID> HTTPメソッド : POST 入力パラメータ: (SCS cookie) 正常に実行された結果: (SCS cookie)、空のオブジェクト
delete_threat	アクション: 脅威のIDである <threat ID>で指定された脅威を含むファイルを削除します。 URI: /api/10.2/delete_threat/ <threat ID> HTTPメソッド : POST 入力パラメータ: (SCS cookie) 正常に実行された結果: (SCS cookie)、空のオブジェクト
ignore_threat	アクション: 脅威のIDである <threat ID>で指定された脅威を無視します。 URI: /api/10.2/ignore_threat/ <threat ID> HTTPメソッド : POST 入力パラメータ: (SCS cookie) 正常に実行された結果: (SCS cookie)、空のオブジェクト
quarantine_threat	アクション: 脅威のIDである <threat ID>で指定された脅威を隔離します。 URI: /api/10.2/quarantine_threat/ <threat ID>



APIコマンド	説明
	HTTPメソッド : POST 入力パラメータ : (SCS cookie) 正常に実行された結果 : (SCS cookie)、空のオブジェクト

指定されたアプリケーションで見つかったそれぞれの脅威には、一意の整数で表されたID <threat ID>があります。すべてのIDのリストはthreatsコマンドによって返されます。threat_info、cure_threat、delete_threat、ignore_threat、およびquarantine_threatコマンドでは、threatsコマンドが返すIDのみが許容されます。

アクション履歴を含む、指定された脅威に関するすべての情報は、threat_infoリクエストを使用して取得できます。情報はFileThreatオブジェクトとして返されます。

JSONオブジェクトの説明

1) FileThreatは、次のデータを含むオブジェクトです。

```
{
  "threat_id": number, //Threat identifier
  "detection_time": UNIXTime, //Time when the threat was detected
  "report": ScanReport, //Report about scanning the file
  "stat": FileStat, //Information about the file
  "origin": string, //Name of the component that detected the threat
  "origin_pid": number, //PID of the component that detected the threat
  "task_id": number, //Identifier of the scanning task
  //in the scan engine
  "history": ActionResult[] //History of actions applied to the threat (an
array)
}
```

reportフィールドにはScanReportオブジェクトが含まれます。statフィールドにはFileStatオブジェクトが含まれ、historyフィールドにはActionResultオブジェクト(ファイルに適用されたアクションの履歴)の配列が含まれます。

2) ScanReport - 脅威が検出されたファイルに関する情報を含むオブジェクト。

```
{
  "object": string, //File system object that contains the threat
  "size": number, //Size (in bytes) of the file that contains the threat
  "virus": VirusInfo[], //List of details about the found
  //threats
  *"error": string, //An error message
  "heuristic_analysis": bool //Flag that shows whether heuristic
  //analysis was used
}
```

アスタリスク(*)のパラメータは任意です。

virusフィールドは、検出されたすべての脅威に関する情報を含むVirusInfoオブジェクトの配列です。errorフィールドは、エラーが発生した場合にのみ表示されます。



3) FileStatは、ファイル統計を含むオブジェクトです。

```
{
  "dev": number, //Device containing the file
  "ino": number, //The file inode number
  *"size": number, //Size of the file
  *"uid": User, //User ID of the file's owner
  *"gid": Group, //Group ID of the owning group
  *"mode": number, //The mode of access to the file
  *"mtime": UNIXTime, //Date/time when the file was last modified
  *"ctime": UNIXTime //Date/time when the file was created
  *"rsrc_size": number, //
  *"finder_info": string, //
  *"ext_finder_info": string, //
  *"uchg": string, //
  *"volume_name": string, //Volume name
  *"volume_root": string, //Root (mount point) of the volume
  *"xattr": XAttr[] //Extended information about the file
}
```

アスタリスク(*)のパラメータは任意です。

xattrフィールドには、XAttrオブジェクトの配列が含まれています。このオブジェクトには、nameおよびvalueの2つの文字列タイプのフィールドがあります。uidフィールドとgidフィールドにはそれぞれユーザーオブジェクトとグループオブジェクトが含まれており、これらのオブジェクトにはそれぞれファイルの所有者とファイルを所有しているグループに関する情報が含まれています。これらのオブジェクトにはそれぞれ次の2つのフィールドがあります。

- uid(gid) - ユーザー(グループ)のID(数値)
- username(groupname) - ユーザー(グループ)の名前(文字列)

4) ActionResultは、ファイルに適用されたアクションとその結果に関する情報を含むオブジェクトです。

```
{
  "action": string, //The action applied
  "action_time": UNIXTime, //Date/time when the action was applied
  "result": string, //Result of applying the action
  "cure_report": ScanReport //Report about applying the action
}
```

cure_threat、delete_threat、ignore_threat、およびquarantine_threatコマンドは、正常に実行されると空のオブジェクトを返します。リクエストされたアクションが失敗した場合は、Errorオブジェクトが返されます。

6. 隔離の管理

隔離オブジェクトを管理するため、HTTP APIには次のコマンドが用意されています。

APIコマンド	説明
quarantine	アクション: 隔離されたオブジェクトのIDの一覧を表示します。 URI: /api/10.2/quarantine/



APIコマンド	説明
	<p>HTTPメソッド: GET</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: (SCS cookie)、QuarantineIdオブジェクト(隔離内のオブジェクト)の配列</p>
qentry_info	<p>アクション: 隔離オブジェクトのIDである <entry ID>で指定された隔離オブジェクトに関する情報を取得します。</p> <p>URI: /api/10.2/qentry_info/ <entry ID></p> <p>HTTPメソッド: GET</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: (SCS cookie)、QEntryオブジェクト</p>
cure_qentry	<p>アクション: 隔離オブジェクトのIDである <entry ID>で指定された隔離オブジェクトの修復を試みます。</p> <p>URI: /api/10.2/cure_qentry/ <entry ID></p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: (SCS cookie)、空のオブジェクト</p>
delete_qentry	<p>アクション: 隔離オブジェクトのIDである <entry ID>で指定された隔離オブジェクトを削除します。</p> <p>URI: /api/10.2/delete_qentry/ <entry ID></p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: (SCS cookie)、空のオブジェクト</p>
restore_qentry	<p>アクション: 隔離オブジェクトのIDである <entry ID>で指定された隔離オブジェクトを元の場所に復元します。</p> <p>URI: /api/10.2/restore_qentry/ <entry ID></p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: (SCS cookie)、空のオブジェクト</p>

それぞれの隔離オブジェクトには一意のIDがあります。[QuarantineId](#)として表されるIDのリストは、`quarantine`コマンドによって返されます。IDは`chunk_id`と`entry_id`の2つの部分で構成されます。



JSONオブジェクトの説明

1) QuarantineIdは、隔離オブジェクトの2つの部分からなるIDの両方の部分を含むオブジェクトです。

```
{
  "chunk_id": string,
  "entry_id": string
}
```

これら2つのフィールドが一体となって隔離オブジェクトのIDを構成します。qentry_info、cure_qentry、delete_qentry、またはrestore_qentryコマンドを使用して隔離オブジェクトにアクションを適用するには、隔離オブジェクトの一般的なIDである<entry ID>を<entry_id>@<chunk_id>の形式で指定する必要があります。qentry_infoコマンドを使用すると、指定されたIDとともに隔離オブジェクトに関する詳細情報を取得できます。このコマンドはQEntryタイプのオブジェクトを返します。

2) QEntry - 隔離オブジェクトに関する情報を含むオブジェクト。

```
{
  "entry_id": string, //Parts of the identifier of
  *"chunk_id": string, //this quarantined object
  *"quarantine_dir": string, //Quarantine directory
  "restore_path": string, //path where the quarantined
  //object will be restored
  "creation_time": number, //Date/time of moving to quarantine
  //(in UNIX time)
  "report": ScanReport, //Report about scanning the object
  //(see ScanReport described above)
  "stat": FileStat, //Statistical information about the file
  //(see FileStat described above)
  *"history": QEntryOperation[], //History of operations performed on the
  object
  *"who": RemoteUser, //The remote owner of the file (if
  //the file was quarantined from a file server
  //storage)
  *"detection_time": number, //Date/time of detecting the threat
  *"origin": string, //Component that detected the threat
}
```

アスタリスク(*)のパラメータは任意です。

reportフィールドにはScanReportオブジェクトが含まれます。statフィールドにはFileStatオブジェクトが含まれ、historyフィールドには、隔離オブジェクトに適用されたアクションの履歴が含まれます。各アクションエントリはQEntryOperationオブジェクトによって記述されます。オプションのwhoフィールドには、削除されたユーザーに関する情報がRemoteUserオブジェクトの形式で含まれます。

3) QEntryOperationは、隔離オブジェクトに適用された操作に関するデータを含むオブジェクトです。

```
{
  "action": string, //Operation performed on the object
  //(see the possible values below)
  "action_time": number, //Date/time when the operation was performed
  (UNIX Time)
  "result": string, //Error when trying to perform the operation (a code
  //EC_XXX)
```



```
*"restore_path": string, //path for restoring the quarantined object
//(if action = "QENTRY_ACTION_RESTORE")
*"rescan_report": ScanReport //Report about rescanning (if
//action = "QENTRY_ACTION_RESCAN")
}
```

アスタリスク(*)のパラメータは任意です。

actionフィールドには、以下の値を指定できます。

- QENTRY_ACTION_DELETEは、隔離オブジェクトの削除を試みます。
- QENTRY_ACTION_RESTOREは、隔離オブジェクトの復元を試みます。
- QENTRY_ACTION_RESCANは、隔離オブジェクトの再スキャンを試みます。
- QENTRY_ACTION_CUREは、隔離オブジェクトの修復を試みます。

4) RemoteUserは、ファイルを所有するリモートユーザーに関する情報を含むオブジェクトです(ファイルがファイルサーバーストレージから隔離に再配置された場合)。

```
{
  *"ip": string, //IP-address of the user
  *"user": string, //User name
  *"domain": string //Domain of the user
}
```

アスタリスク(*)のパラメータは任意です。

cure_gentry、delete_gentry、restore_gentryコマンドの実行が成功すると、空のオブジェクトが返されます。隔離オブジェクトに対して要求された操作がエラーで終了した場合(たとえば、ファイルを復元できなかった場合)、空のオブジェクトの代わりにErrorオブジェクトが返されます。

7. HTTP APIの使用例

HTTP APIの動作をテストするには、curlユーティリティを使用します。API呼び出しの一般的なフォーマットは以下のとおりです。

```
$ curl https://<HTTPD.AdminListen>/<HTTP API URI> -k -X <HTTP method name>
[-H 'Content-Type: application/json' --data-binary '@<file of the JSON object>']
[-c <cookie file> [-b <cookie file>]] [> <file of the result>]
```

- -kオプションでは、curlがSSL証明書を確認しないように指定します。
- -Xオプションでは、使用するHTTPメソッド(GETまたはPOST)を指定します。
- -Hオプションは、Content-Type: application/jsonヘッダーの追加に使用します。
- --data-binary(または-d)オプションは、テキストファイルに保存されたJSONオブジェクトをリクエストに追加するために使用します。
- SCSを使用して承認を得る場合、送受信したSCS cookieを含むファイルをそれぞれ-bと-cのパラメータで指定する必要があります。

curlオプションの詳細な説明については、manページを参照してください(curl --helpまたはman curlコマンドを実行してください)。

1. ユーザー名とパスワード(SCS用)を指定して、クライアントを認証および承認する。



JSON形式のAuthOptionsオブジェクトがあらかじめuser.jsonというファイルに書き込まれている必要があります。例:

```
{"user": "<ユーザー名>", "password": "<パスワード>"}
```

リクエスト:

```
$ curl https://127.0.0.1:4443/api/10.2/login -k -X POST -H 'Content-Type: application/json' --data-binary '@user.json' -c cookie.file
```

レスポンス:

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 2
Set-Cookie:
DWTOKEN=6QXy4wn_JGov9A1GohWP_kvMK3dN6ccKegjNgKcmHpb_AqSrHg9cNX_yFJhxDgr|
MTQ2Mjg3Mzg4NQ==|cWd4Ow==|GywBUVOhU4w2LF_BKT5frg==|
kR_rip5nrpxWjJ2dfZ7Xfmvi3rE=; Secure; HttpOnly; Max-Age: 900; Path=/
Pragma: no-cache

{}
```

Set-Cookieヘッダーフィールドには、それ以降のHTTP APIへのすべてのリクエストで使用する必要があるSCS cookieが含まれています。認証と承認が成功した場合、レスポンスの本文には空のオブジェクトが含まれています。ユーザーが承認されなかった場合は、次のようなErrorオブジェクトが返されます。

```
HTTP/1.0 403 Forbidden
Content-Type: application/json
Content-Length: 35
Pragma: no-cache

{"error":{"code":"EC_AUTH_FAILED"}}
```

2. IDがICである脅威に関する情報を取得する。

リクエスト:

```
$ curl https://127.0.0.1:4443/api/10.2/threat_info/1 -k -X GET -c cookie.file -b cookie.file
```

レスポンス:

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 574
Set-Cookie: DWTOKEN=<...>;
Secure; HttpOnly; Max-Age: 900; Path=/
Pragma: no-cache

{"threat_id":1,"detection_time":1462881660,
"report":{"object":"/sites/site1/eicar.com.txt","size":68,"packer":[],
"virus":[{"type":"SE_KNOWN_VIRUS","name":"EICAR Test File (NOT a
Virus!)"}]},
"heuristic_analysis":true,"core_fingerprint":"0D2DD5A869DAB7AE354153A4D5F
70F45",
"item":[],"log":[],"user_time":0,"system_time":0},"stat":
```



```
{"dev":2049,"ino":898,
"size":68,"uid":{"uid":1000,"username":"user"},"gid":
{"gid":1000,"groupname":"user"},
"mode":33204,"mtime":1441028214,"ctime":1460738554,"xattr":[],
"origin":"APP_COMMAND_LINE_TOOL","origin_pid":2726,"task_id":1,"history":
[]}
```

3. IDがICである脅威を隔離へ移動する。

リクエスト:

```
$ curl -v -c cookie.jar -b cookie.jar -k -X POST -H 'Content-
Type:application/json'
https://127.0.0.1:4443/api/10.2/quarantine_threat/1
```

レスポンス:

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 2
Set-Cookie: DWToken=<...>; Secure; HttpOnly; Max-Age: 900; Path=/
Pragma: no-cache

{}
```

4. 指定されたIDを持つ隔離オブジェクトに関する情報を表示する。

リクエスト:

```
$ curl -v -k -X GET -c cookie.jar -b cookie.jar
https://127.0.0.1:4443/api/10.2/qentry_info/3070d3ce-7b6e-4143-9d9f-
89ba3473a781@801:2108d
```

レスポンス:

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 781
Set-Cookie: DWToken=<...>; Secure; HttpOnly; Max-Age: 900; Path=/
Pragma: no-cache

{"entry_id":"3070d3ce-7b6e-4143-9d9f-
89ba3473a781","chunk_id":"3830313A3231303864",
"quarantine_dir":"2F686F6D652F757365722F2E636F6D2E64727765622E71756172616
E74696E65",
"restore_path":"2E2E2F7473742F65696361722E636F6D2E747874","creation_time"
:1462888884,
"report":{"object":"/home/user/tst/eicar.com.txt","size":68,"packer":[],
"virus":[{"type":"SE_KNOWN_VIRUS","name":"EICAR Test File (NOT a
Virus!)"}]},
"heuristic_analysis":true,"core_fingerprint":"467CD4C6D423C55448B71CD5B81
52776",
"item":[],"log":[],"user_time":0,"system_time":0},"stat":
{"dev":2049,"ino":898,
"size":68,"uid":{"uid":1000,"username":"user"},"gid":
{"gid":1000,"groupname":"user"},
```




```
"mode":33204,"mtime":1441028214,"ctime":1462888421,"xattr":[],"history":
[],
"detection_time":1462888667,"origin":"APP_COMMAND_LINE_TOOL"}
```

5. 設定を変更する: Dr.Web CloudDを無効にする。

JSON形式のLexMapオブジェクトがあらかじめlexmap_ls_off.jsonというファイルに書き込まれている必要があります。

```
{"option":[{"key":"Root","map":{"option":
[{"key":"UseCloud","value":{"item":["no"]}}]}}]}
```

リクエスト:

```
$ curl -v -k -c cookie.jar -b cookie.jar -X POST -H 'Content-Type:
application/json' --data-binary '@lexmap_ls_off.json'
https://127.0.0.1:4443/api/10.2/set_lexmap
```

レスポンス:

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 58
Set-Cookie: DWToken=<...>; Secure; HttpOnly; Max-Age: 900; Path=/
Pragma: no-cache

{"item":[{"option":"Root.UseCloud","result":"EC_OK"}]}
```

6. 設定を変更する: Dr.Web CloudDを有効にする。

JSON形式のLexMapオブジェクトがlexmap_ls_on.jsonという名前のファイルに保存されている必要があります。

```
{"option":[{"key":"Root","map":{"option":
[{"key":"UseCloud","value":{"item":["yes"]}}]}}]}
```

リクエスト:

```
$ curl -v -k -c cookie.jar -b cookie.jar -X POST -H 'Content-Type:
application/json' --data-binary '@lexmap_ls_on.json'
https://127.0.0.1:4443/api/10.2/set_lexmap
```

レスポンス:

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 58
Set-Cookie: DWToken=<...>; Secure; HttpOnly; Max-Age: 900; Path=/
Pragma: no-cache

{"item":[{"option":"Root.UseCloud","result":"EC_OK"}]}
```



Dr.Web SNMPD

Dr.Web SNMPDは、SNMPプロトコルを実行するモニタリングシステムにDr.Web for UNIX Internet Gatewaysを統合するよう設計されたSNMPエージェントです。この統合により、Dr.Web for UNIX Internet Gatewaysのコンポーネントのステータスを追跡したり、脅威の検出と駆除に関する統計を収集したりできます。このエージェントのサポートにより、モニタリングシステムまたはSNMPマネージャーに以下の情報が提供されます。

- 任意のDr.Web for UNIX Internet Gatewaysコンポーネントのステータス。
- 検出されたさまざまなタイプの脅威の数 (Dr.Web分類に対応)。

さらに、エージェントは、脅威を検出したときと検出された脅威の駆除が失敗したときにSNMPトラップ通知を送信します。エージェントはSNMPプロトコルバージョン2cおよび3をサポートします。

エージェントが送信できる情報の説明は、Doctor Webによって作成されたMIB (管理情報ベース) の特別なセクションに格納されています。UNIX系オペレーティングシステム用にDr.Webが定義したMIBセクションには、以下の情報が指定されています。

1. 脅威の検出と駆除、Dr.Web for UNIX Internet Gatewaysコンポーネントに関連するエラーに関するSNMPトラップ通知のフォーマット。
2. Dr.Web for UNIX Internet Gateways操作の統計。
3. Dr.Web for UNIX Internet Gatewaysコンポーネントのステータス。

SNMPプロトコルを介して取得できる情報の詳細については、対応する[セクション](#)を参照してください。

動作原理

このセクションの内容

- [概要](#)
- [システムSNMPエージェントとの統合](#)

概要

デフォルトでは、このコンポーネントはDr.Web for UNIX Internet Gatewaysの起動時に自動的に実行されます。実行されると、このコンポーネントはMIB Dr.Webで記述されている構造に従ってデータを構造化し、外部SNMPマネージャーからのデータ受信要求を待機します。このコンポーネントは[Dr.Web ConfigD](#)設定デーモンから、Dr.Web for UNIX Internet Gatewaysのコンポーネントのステータスに関する情報と、検出された脅威に関する通知を直接受信します。

脅威は、Dr.Web for UNIX Internet Gatewaysコンポーネントによるスキャン中にスキャンエンジンによって検出されます。何らかの脅威が検出されると、(この脅威の種類に) 該当するカウントが1つ増え、通知を受信できるすべてのSNMPマネージャーは、検出された脅威について通知するSNMPトラップを受け取ります。



カウンターの収集値 (たとえば、検出された脅威のカウンター) は、Dr.Web SNMPDの起動の間は保存されません。したがって、Dr.Web SNMPDが何らかの理由 (Dr.Web for UNIX Internet Gatewaysの通常の再起動を含む) で再起動されると、収集されたカウンターの値は0にリセットされます。



システムSNMPエージェントとの統合

メインシステムのSNMPエージェントsnmpd (net-snmp) がすでにサーバー上で動作している場合にDr.Web SNMPエージェントを正しく動作させるには、Dr.Web MIBブランチを介したsnmpdからDr.Web SNMPへのSNMPリクエスト送信を設定します。そのためには、次の行を追加してsnmpd設定ファイル(GNU/Linuxの場合は、通常/etc/snmp/snmpd.conf)を編集します。

```
proxy -v <version> -c <community> <address>:<port> <MIB branch>
```

各パラメータは次のとおりです。

- <version> - 使用中のSNMPバージョン(2c、3)
- <community> - Dr.Web SNMPDによって使用される「コミュニティストリング」
- <address>:<port> - Dr.Web SNMPDによってリッスンされるネットワークソケット
- <MIB branch> - Dr.Webが使用する変数とSNMPトラップの[説明](#)を含むMIBブランチのOID(OIDは .1.3.6.1.4.1.29690)

Dr.Web SNMPエージェントをデフォルト設定で使用している場合、追加する行は以下のようになります。

```
proxy -v 2c -c public localhost:50000 .1.3.6.1.4.1.29690
```

この場合、ポート161はシステムの標準snmpdによって使用されるため、ListenAddress[パラメータ](#)でDr.Web SNMPD用に別のポートを指定する必要があります(この例では、50000)。



コマンドライン引数

OSのコマンドラインからDr.Web SNMPDを起動するには、次のコマンドを使用します。

```
$ <opt_dir>/bin/drweb-snmpd [<parameters>]
```

Dr.Web SNMPDは次のオプションを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了します。 短縮形：-h 引数：なし
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了します。 短縮形：-v 引数：なし

例：

```
$ /opt/drweb.com/bin/drweb-snmpd --help
```

このコマンドは、Dr.Web SNMPDに関する簡単なヘルプ情報を出力します。

スタートアップノート

このコンポーネントは、自律モードで(他のコンポーネントから自律的に)OSのコマンドラインから直接起動することはできません。必要に応じてDr.Web ConfigD設定デーモンによって自動的に起動されます(原則として、OSの起動時)。コンポーネントの動作を管理するには、Dr.Web for UNIX Internet Gateways用のコマンドラインベース管理ツールDr.Web Ctlを使用できます(これはdrweb-ctlコマンドを使用して呼び出されます)。



コマンドラインから製品のこのコンポーネントに関するドキュメントを要求するには、`man 1 drweb-snmpd`コマンドを使用します。

設定パラメータ

このコンポーネントは、Dr.Web for UNIX Internet Gatewaysの統合された設定ファイルの[SNMPD]セクションで指定されている設定パラメータを使用します。

セクションには以下のパラメータが含まれています。

パラメータ	説明
LogLevel	コンポーネントのロギングレベル。



パラメータ	説明
<i>{logging level}</i>	パラメータの値が指定されていない場合は、[Root] セクション のDefaultLogLevelパラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行ファイルへのパス。 デフォルト値: <opt_dir>/bin/drweb-snmpd <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-snmpd。• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-snmpd。
Start <i>{Boolean}</i>	Dr.Web ConfigD 設定デーモンによってコンポーネントを起動するかどうかを指定します。 このパラメータにYes値を指定すると、設定デーモンはただちにコンポーネントを開始します。また、No値を指定すると、設定デーモンはただちにコンポーネントを終了します。 デフォルト値: No
RunAsUser <i>{UID user name}</i>	コンポーネントの実行に必要な権限を有するユーザー。このユーザー名は、ユーザーのUIDまたはユーザーのログインとして指定できます。ユーザー名が数字で構成されている場合(つまり、数字のUIDに似ている場合)は、「name:」というプレフィックスを付けて指定します。たとえば、 RunAsUser = name:123456です。 ユーザー名が指定されていない場合、コンポーネント操作は開始後にエラーが発生して終了します。 デフォルト値: drweb
ListenAddress <i>{address}</i>	クライアント接続(SNMPマネージャー)を待機するDr.Web SNMPDがリッスンするアドレス(IPアドレスとポート)。 snmpdとのインタラクションには、標準ポート(161)とは異なるポートの指定と、snmpdにプロキシ用の 設定を行う 必要があります。 デフォルト値: 127.0.0.1:161
SnmVersion <i>{V2c / V3}</i>	SNMPプロトコルの現在のバージョン(<i>SNMPv2c</i> または <i>SNMPv3</i>)。 デフォルト値: V2c
V3EngineId <i>{string}</i>	<i>SNMPv3のエンジンID</i> の識別子(文字列)(RFC 3411 に準拠)。 デフォルト値: 800073FA044452574542



パラメータ	説明
TrapReceiver {address list}	<p>Dr.Web for UNIX Internet Gatewaysのコンポーネントが脅威を検出した後に、Dr.Web SNMPDによってSNMPトラップ通知が送信されるアドレスのリスト (IPアドレスとポート)。</p> <p>リストをパラメータ値として指定できます。リストの値は、コンマ (引用符内の各値) で区切る必要があります。パラメータはセクションで複数回指定できます (この場合、そのすべての値が1つのリストにまとめられます)。</p> <p>例: ソケット192.168.0.1:1234および10.20.30.45:5678をリストに追加します。</p> <ol style="list-style-type: none">設定ファイルに値を追加します。<ul style="list-style-type: none">1つの文字列に2つの値: <pre>セクション[SNMPD] TrapReceiver = "192.168.0.1:1234", "10.20.30.45:5678"</pre>2つの文字列 (文字列ごとに1つの値): <pre>[SNMPD] TrapReceiver = 192.168.0.1:1234 TrapReceiver = 10.20.30.45:5678</pre>drweb-ctl cfsetコマンドを使用して値を追加します。 <pre># drweb-ctl cfset SNMPD.TrapReceiver -a 192.168.0.1:1234 # drweb-ctl cfset SNMPD.TrapReceiver -a 10.20.30.45:5678</pre> <p>デフォルト値: (未設定)</p>
V2cCommunity {string}	<p>Dr.WebのMIB変数が読み取りアクセスされたときに、SNMPマネージャー (SNMPv2cプロトコル) を認証するための文字列「SNMP read community」。</p> <p>SnmVersion = V2cの場合、このパラメータが使用されません。</p> <p>デフォルト値: public</p>
V3UserName {string}	<p>Dr.WebのMIB変数が読み取りアクセスされたときに、SNMPマネージャー (SNMPv3プロトコル) を認証するためのユーザー名。</p> <p>SnmVersion = V3の場合、このパラメータが使用されません。</p> <p>デフォルト値: noAuthUser</p>
V3Auth {SHA(<pwd>) MD5(<pwd>) None}	<p>Dr.WebのMIB変数が読み取りアクセスされたときに、SNMPマネージャー (SNMPv3プロトコル) を認証する方法。</p>



パラメータ	説明
	<p>使用可能な値：</p> <ul style="list-style-type: none">• SHA (<PWD>) - パスワードのSHAハッシュが使用されます (<PWD>文字列)。• MD5 (<PWD>) - パスワードのMD5ハッシュが使用されます (<PWD>文字列)。• None - 認証は無効になります。 <p>ここで、<PWD>はプレーンテキストのパスワードです。</p> <p>コマンドラインからパラメータ値を指定する場合、シェルによってはスラッシュ記号\を使用した角括弧のエスケープを必要とする場合があります。</p> <p>例：</p> <ol style="list-style-type: none">1. 設定ファイル内のパラメータ値： V3Auth = MD5(123456)2. drweb-ctl cfset コマンドを使用して、コマンドラインから同じパラメータ値を指定する場合： drweb-ctl cfset SNMPD.V3Auth MD5\ (123456\) <p>SnmpVersion = V3の場合、このパラメータが使用されません。</p> <p>デフォルト値 : None</p>
V3Privacy {DES(<secret>) AES128(<secret>) / None}	<p>SNMPメッセージの暗号化方式 (SNMPv3プロトコル)。</p> <p>使用可能な値：</p> <ul style="list-style-type: none">• DES (<secret>) - DES暗号化アルゴリズム。• AES128 (<secret>) - AES128暗号化アルゴリズム。• None - SNMPメッセージは暗号化されません。 <p>ここで、<secret>は、マネージャーとエージェントが共有するシークレットキーです (プレーンテキスト)。</p> <p>コマンドラインからパラメータ値を指定する場合、シェルによってはスラッシュ記号\を使用した角括弧のエスケープを必要とする場合があります。</p> <p>例：</p> <ol style="list-style-type: none">1. 設定ファイル内のパラメータ値： V3Privacy = AES128(supersecret)2. drweb-ctl cfset コマンドを使用して、コマンドラインから同じパラメータ値を指定する場合： drweb-ctl cfset SNMPD.V3Privacy AES128\ (supersecret\) <p>SnmpVersion = V3の場合、このパラメータが使用されません。</p>



パラメータ	説明
	デフォルト値 : None

SNMPモニタリングシステムとの統合

Dr.Web SNMPエージェントは、SNMPプロトコル、バージョン2cまたは3を使用するモニタリングシステムのデータプロバイダーとして機能します。制御に使用できるデータのリストとデータ構造は、Dr.Web for UNIX Internet Gatewaysに付属のDr.Web MIB記述ファイルDRWEB-SNMPD-MIB.txtに記述されています。このファイルは、ディレクトリ<opt_dir>/share/drweb-snmpd/mibsにあります。

簡単に設定できるように、このコンポーネントには一般的なモニタリングシステム用の設定テンプレートが付属しています。

- [Munin](#)
- [Nagios](#)
- [Zabbix](#)

モニタリングシステム用のカスタマイズテンプレートは、<opt_dir>/share/drweb-snmpd/connectorsディレクトリにあります。

Muninモニタリングシステムとの統合

Muninモニタリングシステムには、モニタリング対象ホストにローカルに存在するクライアントmunin-nodeから統計を収集する中央サーバー(マスター)muninが含まれています。サーバーのリクエストに応じて、各モニタリングクライアントは、サーバーに転送されたデータを提供するプラグイン(プラグイン)を起動することによって、モニタリング対象ホストの動作に関するデータを収集します。

Dr.Web SNMPDとMuninモニタリングシステム間の接続を可能にするために、すぐに利用できるmunin-node用プラグインDr.Webが用意されています。このプラグインは<opt_dir>/share/drweb-snmpd/connectors/munin/pluginsディレクトリにあります。このプラグインは、次の2つのグラフの作成に必要なデータを収集します。

- 検出された脅威の数。
- ファイルのスキャン統計情報
- メールメッセージのスキャン統計(Dr.Web MailDコンポーネントでのみメール統計を取得できます。Dr.Web MailDはDr.Web for UNIX Internet Gatewaysには含まれていません)。

これらのプラグインは、SNMPプロトコルバージョン1、2c、3をサポートしています。これらのテンプレートプラグインに基づいて他のプラグインを作成すれば、Dr.Web SNMPD経由でDr.Web for UNIX Internet Gatewaysのコンポーネントのステータスをポーリングできます。

<opt_dir>/share/drweb-snmpd/connectors/muninディレクトリには、以下のファイルがあります。

ファイル	説明
plugins/snmp__drweb_malware	ホスト上のDr.Web for UNIX Internet Gatewaysによって検出された脅威の数を収集するために、SNMP経由で



ファイル	説明
	Dr.Web SNMPDをポーリングするためのmunin-nodeプラグイン。
plugins/snmp__drweb_filecheck	ホスト上のDr.Web for UNIX Internet Gatewaysによってスキャンされたファイルの統計を収集するために、SNMP経由でDr.Web SNMPDをポーリングするためのmunin-nodeプラグイン。
plugin-conf.d/drweb.cfg	Dr.Webプラグインのmunin-node設定の例（環境変数用）。

Muninにホストを接続する

この説明では、Muninモニタリングシステムがモニタリングサーバーにすでにデプロイされており、モニタリング対象ホストにはDr.Web SNMPDがインストール済みでmunin-nodeとともに機能している（コンポーネントはsnmpdとともに[プロキシ](#)モードで機能する）と想定しています。

1. モニタリング対象ホストの設定

- snmp__drweb_*ファイルを、プラグインライブラリmunin-nodeがあるディレクトリにコピーします（ディレクトリはOSによって異なります）。たとえば、Debian/Ubuntuオペレーティングシステムであれば、パスは/usr/share/munin/pluginsとなります。
- 提供されているDr.Webプラグインを接続して、munin-nodeを設定します。これを行うには、munin-nodeと一緒に配布されるmunin-node-configureユーティリティを使用します。

次は、コマンドの例です。

```
$ munin-node-configure --shell --snmp localhost
```

端末画面に、プラグインに必要なシンボリックリンクを作成するためのコマンドのリストを表示します。コピーして、コマンドラインで実行します。指定されたコマンドでは、次のことを前提としています。

- 1) munin-nodelは、Dr.Web SNMPDがインストールされているのと同じホストにインストールされている。インストール先が異なる場合は、localhost値ではなく、モニタリング対象ホストの適切なFQDNまたはIPアドレスを指定してください。
 - 2) Dr.Web SNMPDはSNMPバージョン2cを使用する。他のバージョンの場合は、munin-node-configureコマンドで適切なSNMPバージョンを指定してください。このコマンドには、プラグインを柔軟に設定するための引数がいくつかあります。たとえば、SNMPプロトコルのバージョン、モニタリング対象ホストでSNMPエージェントがリスンしているポート、コミュニティストリングの実際の値などを指定できます。必要に応じて、munin-node-configureコマンドのマニュアルを参照してください。
- 必要であれば、munin-node用にインストールしたDr.Webプラグインを実行する環境のパラメータ値を定義（または再定義）します。環境パラメータとして、値コミュニティストリングが使用されます。これは、SNMPエージェントなどが使用するポートです。これらのパラメータは、ファイル/etc/munin/plugin-conf.d/drwebに定義する必要があります（必要に応じて作成します）。このファイルの例として、提供されているファイルdrweb.cfgを使用します。
 - munin-node設定ファイル(munin-node.conf)で、モニタリング対象のパラメータの値を受け取るためにmuninサーバー（マスター）をmunin-nodelに接続できるホストのすべてのIPアドレスを含めるための正規表現を指定します。たとえば、次のようになります。



```
allow ^10\.20\.30\.40$
```

この場合、IPアドレス10.20.30.40のみがホストパラメータを受信できます。

- たとえば、次のコマンドを使用してmunin-nodeを再起動します。

```
# service munin-node restart
```

2. Muninサーバー(マスター)の設定

モニタリング対象ホストのアドレスと識別子をMunin設定ファイル`munin.conf`に追加します。このファイルは、デフォルトでは`/etc`ディレクトリにあります(Debian/Ubuntuオペレーティングシステムでは`/etc/munin/munin.conf`になります)。

```
[ <ID>; <hostname>. <domain> ]  
address <host IP address>  
use_node_name yes
```

ここで、`<ID>`は表示されるホストの識別子、`<hostname>`はホストの名前、`<domain>`はドメインの名前、`<host IP address>`はホストのIPアドレスです。

Muninモニタリングシステムの設定に関する公式マニュアルについては、<http://guide.munin-monitoring.org/en/latest/>を参照してください。

Zabbixモニタリングシステムとの統合

Dr.Web SNMPDとZabbixモニタリングシステム間の接続を確立するために必要なファイルテンプレートは、`<opt_dir>/share/drweb-snmpd/connectors/zabbix`ディレクトリにあります。

ファイル	説明
<code>zbx_drweb.xml</code>	Dr.Web for UNIX Internet Gatewaysがインストールされているモニタリング対象ホストを説明するためのテンプレート
<code>snmptt.drweb.zabbix.conf</code>	SNMPトラップハンドラーである <code>snmptt</code> ユーティリティの設定

モニタリング対象ホストの機能を説明するためのテンプレート:

- カウンター(*Zabbix*の用語では「アイテム」)の説明。デフォルトでは、テンプレートはSNMP v2で使用されるように設定されています。
- 既存のグラフのセット: スキャンされたファイルの数と検出された脅威のタイプ別の分布。



Zabbixにホストを接続する

この説明では、Zabbixモニタリングシステムがモニタリングサーバーにすでにデプロイされており、モニタリング対象ホストにはDr.Web SNMPDがインストール済みで機能している(コンポーネントはsnmpdとともに**プロキシ**モードで機能する)と想定しています。さらに、モニタリング対象ホストからSNMPトラップ通知(保護対象サーバーでDr.Web for UNIX Internet Gatewaysによって検出された脅威に関する通知を含む)を受信する場合は、モニタリングサーバーにnet-snmpパッケージをインストールします(標準ツールのsnmpdおよびsnmptrapdが使用されます)。

1. Zabbix Webインターフェースの設定 → テンプレートタブで、`<opt_dir>/share/drweb-snmppd/connectors/zabbix/zbx_drweb.xml`ファイルからモニタリング対象ホストのテンプレートをインポートします。
2. モニタリング対象ホストを適切なリストに追加します(ホスト → ホストの作成)。ホストの適切なパラメータとSNMPインターフェースの設定を指定します(ホストのdrweb-snmppdとsnmpdの設定と一致する必要があります)。
 - ホストタブ:
 - ホスト名: `drweb-host`
 - 表示名: `DRWEB_HOST`
 - グループ: `Linux servers`を選択します
 - SNMPインターフェース**: 追加をクリックして、Dr.Web SNMPDによって使用されるIPアドレスとポートを指定します(Dr.Web SNMPDはローカルホストで動作すると見なされるため、デフォルトではアドレス `127.0.0.1`とポート `161`が指定されています)。
 - テンプレートタブ:
 - 追加を押し、`DRWEB`を確認し、選択を押しします。
 - マクロタブ:
 - マクロ: `{${SNMP_COMMUNITY}}`
 - 値: SNMP V2cに「read community」を指定します(デフォルトでは、`public`)。
 - 保存をクリックします。
 - 注意: `{${SNMP_COMMUNITY}}`マクロは、ホストテンプレートで直接指定できます。
3. テンプレートがモニタリング対象ホストにバインドされた後、SNMP設定が正しく指定されていれば、Zabbixモニタリングシステムはテンプレートのカウンター(アイテム)のデータ収集を開始します。収集されたデータは、監視データ → 最新データと監視データ → グラフに表示されます。
4. Dr.Web SNMPDからSNMPトラップ通知を収集するために、特別なアイテム `drweb-traps`が使用されます。受信したSNMPトラップ通知のログは、監視データ → 最新データ → **drweb-traps** → ヒストリページで利用できます。Zabbixは通知を収集するために、net-snmpパッケージの標準ツールsnmpdとsnmptrapdを使用します。Dr.Web SNMPDからSNMPトラップ通知を受信するためのツールの設定方法については、以下を参照してください。
5. 必要に応じて、Dr.Web SNMPDからのSNMPトラップ通知の受信時に状態を変更するトリガーを設定できます。状態の変更は、適切な通知を生成するためのイベントソースとして使用できます。以下の例は、トリガーの設定式を示しています。この式は**trigger expression**フィールドで指定されます。



デフォルトでは、インポートされた `DRWEB`テンプレートはSNMP v2用に設定されています。他のバージョンのSNMPを使用する場合は、該当するページでテンプレートに必要な編集を行います。



- Zabbixバージョン2.xの場合:

```
{TRIGGER.VALUE}=0 &
{DRWEB:snmptrap[.*\1\.3\.6\.1\.4\.1\.29690\..*].nodata(60)}=1 ) |
({TRIGGER.VALUE}=1 &
{DRWEB:snmptrap[.*\1\.3\.6\.1\.4\.1\.29690\..*].nodata(60)}=0)
```

- Zabbixバージョン3.xの場合:

```
({TRIGGER.VALUE}=0 and {drweb-host:snmptrap[".29690."].nodata(60)}=1 ) or
({TRIGGER.VALUE}=1 and {drweb-host:snmptrap[".29690."].nodata(60)}=0 )
```

Dr.Web SNMPDからのSNMPトラップ通知のログが1分以内に更新された場合、イベントがトリガーされます(値が1に設定されます)。ログが次の1分以内に更新されなかった場合、トリガーの値は再び0に設定されます。

深刻度では、このトリガーの通知タイプを未分類とは異なるものにするをお勧めします(例: 警告)。

ZabbixのSNMPトラップ通知の受信を設定する

1. モニタリング対象ホストのDr.Web SNMPDの設定(TrapReceiverパラメータ)で、Zabbixが動作しているホストでsnmptrapdがリスンするアドレスを指定する必要があります。次に例を示します。

```
SNMPD.TrapReceiver = 10.20.30.40:162
```

2. snmptrapdの設定ファイル(snmptrapd.conf)に、同じアドレスと、受信したSNMPトラップ通知を処理するアプリケーションを指定します(この例ではsnmptthandler、snmpttコンポーネント)。

```
snmpTrapdAddr 10.20.30.40:162
traphandle default /usr/sbin/snmptthandler
```

Dr.Web SNMPDによって送信されたSNMPトラップをsnmpttが不明なものとして破棄しないように、ファイルに次の文字列を追加します。

```
outputOption n
```

3. snmptthandlerコンポーネントは、Zabbixのホストテンプレートに設定されている正規表現(アイテムdrweb-trapsエレメント)に対応する指定された形式に従って、受信したSNMPトラップ通知をディスクのファイルに保存します。保存された通知のSNMPトラップフォーマットは、<opt_dir>/share/drweb-snmppd/connectors/zabbix/snmptt.drweb.zabbix.conf.ファイルで指定します。ファイルは、/etc/snmpにコピーする必要があります。
4. さらに、フォーマットファイルへのパスをsnmptt.iniに指定する必要があります。

```
[TrapFiles]
# A list of snmptt.conf files (this is NOT the snmptrapd.conf file).
# The COMPLETE path and filename. Ex: '/etc/snmp/snmptt.conf'
snmptt_conf_files = <<END
/etc/snmp/snmptt.conf
/etc/snmp/snmptt.drweb.zabbix.conf
END
```

その後、デーモンモードで起動している場合はsnmpttを再起動します。



5. Zabbixサーバーの設定ファイル(zabbix-server.conf)で、次の設定を指定します(または、すでに指定されているかどうかを確認します)。

```
SNMPTrapperFile=/var/log/snmpd/snmpd.log
StartSNMPTrapper=1
```

ここで、/var/log/snmpd/snmpd.logは、受信したSNMPトラップ通知の情報を登録するためにsnmpdが使用するログファイルです。

Zabbixの公式マニュアルについては、<https://www.zabbix.com/documentation/current/en>を参照してください。

Nagiosモニタリングシステムとの統合

Dr.Web SNMPDとNagiosモニタリングシステム間の接続を確立するために必要なファイルとNagiosの設定例は、<opt_dir>/share/drweb-snmpd/connectors/nagiosディレクトリにあります。

ファイル	説明
nagiosgraph/rrdopts.conf-sample	RRD設定ファイルの例
objects/drweb.cfg	drwebオブジェクトを記述する設定ファイル
objects/nagiosgraph.cfg	Nagiosが使用するNagiosgraphによって使用されるグラフ描画のためのコンポーネントの設定ファイル
plugins/check_drweb	Dr.Web for UNIX Internet Gatewaysがインストールされているホストからデータを収集するためのスクリプト
plugins/eventhandlers/submit_check_result	SNMPトラップ通知を処理するためのスクリプト
snmp/snmpd.drweb.nagios.conf	SNMPトラップハンドラーであるsnmpdユーティリティの設定

Nagiosにホストを接続する

この説明では、WebサーバーとグラフィックツールNagiosgraphの設定を含むNagiosモニタリングシステムがモニタリングサーバーにすでにデプロイされており、モニタリング対象ホストにはDr.Web SNMPDがインストール済みで機能している(コンポーネントはsnmpdとともにプロキシモードで機能する)と想定しています。さらに、モニタリング対象ホストからSNMPトラップ通知(保護対象サーバーでDr.Web for UNIX Internet Gatewaysによって検出された脅威に関する通知を含む)を受信する場合は、モニタリングサーバーにnet-snmpパッケージをインストールします(標準ツールのsnmpdおよびsnmptrapdが使用されます)。

現在のマニュアルでは、次のようなパスの規則が使用されています(実際のパスはオペレーティングシステムとNagiosのインストールによって異なります)。

- <NAGIOS_PLUGINS_DIR> - Nagiosプラグインを含むディレクトリ(例:/usr/lib64/nagios/plugins)。
- <NAGIOS_ETC_DIR> - Nagios設定を含むディレクトリ(例:/etc/nagios)。



- `<NAGIOS_OBJECTS_DIR>` - Nagiosオブジェクトを含むディレクトリ (例: `/etc/nagios/objects`)。
- `<NAGIOSGRAPH_DIR>` - Nagiosgraphディレクトリ (例: `/usr/local/nagiosgraph`)。
- `<NAGIOS_PERFDATA_LOG>` - Nagiosがサービスチェックの結果を記録するファイル (`<NAGIOSGRAPH_DIR>/etc/nagiosgraph.conf`の`perflog`ファイルと同じでなければなりません)。このファイルのレコードは`<NAGIOSGRAPH_DIR>/bin/insert.pl`スクリプトによって読み取られ、対応するRRRアーカイブRRDツールに記録されます。

Nagiosを設定する:

1. `check_drweb`ファイルを`<NAGIOS_PLUGINS_DIR>`ディレクトリに、`drweb.cfg`ファイルを`<NAGIOS_OBJECTS_DIR>`ディレクトリにコピーします。
2. 監視対象のDr.Web for UNIX Internet Gatewaysがあるホストを`drweb`グループに追加します。ホストではDr.Web SNMPDが実行されている必要があります。デフォルトでは、このグループには`localhost`のみが追加されます。
3. 必要に応じて、`snmpwalk`ツールを介して`drweb`ホストのDr.Web SNMPDに接続するように指示する`check_drweb`コマンドを編集します。

```
snmpwalk -c public -v 2c $HOSTADDRESS$:161
```

SNMPプロトコルの適切なバージョンとパラメータ(「コミュニティストリング」や認証パラメータなど)の他、ポートを指定します。`$HOSTADDRESS$`変数をコマンドに含める必要があります(この変数は後でコマンドが呼び出されたときに、Nagiosによって正しいホストアドレスに自動的に置き換えられるためです)。このコマンドではOIDは必要ありません。また、実行ファイルへのフルパス(通常は`/usr/local/bin/snmpwalk`)を使用してコマンドを指定することをお勧めします。

4. 次の文字列をファイルに追加して、`<NAGIOS_ETC_DIR>/nagios.cfg`設定ファイルのDrWebオブジェクトを接続します。

```
cfg_file=<NAGIOS_OBJECTS_DIR>/drweb.cfg
```

5. DrWebグラフィック用のRRDツール設定を`rrdopts.conf-sample`ファイルから`<NAGIOSGRAPH_DIR>/etc/rrdopts.conf`ファイルに追加します。
6. Nagiosgraphがまだ設定されていない場合は、その設定に対して次の手順を実行します。
 - `nagiosgraph.cfg`ファイルを`<NAGIOS_OBJECTS_DIR>`ディレクトリにコピーし、`process-service-perfdata-for-nagiosgraph`コマンドで`insert.pl`スクリプトへのパスを編集します。たとえば、次のようになります。

```
$ awk '$1 == "command_line" { $2 = "<NAGIOSGRAPH_DIR>/bin/insert.pl" } { print }' ./objects/nagiosgraph.cfg > <NAGIOS_OBJECTS_DIR>/nagiosgraph.cfg
```

- 次の行を追加して、`<NAGIOS_ETC_DIR>/nagios.cfg`設定ファイルにこのファイルを接続します。

```
cfg_file=<NAGIOS_OBJECTS_DIR>/nagiosgraph.cfg
```

7. `<NAGIOS_ETC_DIR>/nagios.cfg` 設定ファイルのNagiosパラメータの値を確認します。



```
check_external_commands=1
execute_host_checks=1
accept_passive_host_checks=1
enable_notifications=1
enable_event_handlers=1

process_performance_data=1
service_perfddata_file=/usr/nagiosgraph/var/rrd/perfddata.log
service_perfddata_file_template=$LASTSERVICECHECK$||$HOSTNAME$||$SERVICEDE
SC$||$SERVICEOUTPUT$||$SERVICEPERFDATA$
service_perfddata_file_mode=a
service_perfddata_file_processing_interval=30
service_perfddata_file_processing_command=process-service-perfddata-for-
nagiosgraph

check_service_freshness=1
enable_flap_detection=1
enable_embedded_perl=1
enable_environment_macros=1
```

NagiosのSNMPトラップ通知の受信を設定する

1. モニタリング対象ホストのDr.Web SNMPDの設定(TrapReceiverパラメータ)で、Nagiosが動作しているホストでsnmptrapdがリスンするアドレスを指定します。次に例を示します。

```
SNMPD.TrapReceiver = 10.20.30.40:162
```

2. *SNMP*トラップを受信したときに呼び出される `<NAGIOS_PLUGINS_DIR>/eventhandlers/submit_check_result` スクリプトがあるかどうかを確認します。スクリプトが見つからない場合は、`<opt_dir>/share/drweb-snmppd/connectors/nagios/plugins/eventhandlers/` ディレクトリの `submit_check_result` ファイルをこの場所にコピーします。このファイルで、CommandFileパラメータに指定されているパスを変更します。これは、`<NAGIOS_ETC_DIR>/nagios.cfg` ファイルの `command_file` パラメータと同じ値である必要があります。
3. `snmptt.drweb.nagios.conf` ファイルを `/etc/snmp/snmp/` ディレクトリにコピーします。このファイルで、パスを `submit_check_result` に変更します。たとえば、次のようなコマンドを使用します。

```
$ awk '$1 == "EXEC" { $2 =
<NAGIOS_PLUGINS_DIR>/eventhandlers/submit_check_result } { print }'
./snmp/snmptt.drweb.nagios.conf > /etc/snmp/snmp/snmptt.drweb.nagios.conf
```

4. 「`/etc/snmp/snmptt.drweb.nagios.conf`」文字列を `/etc/snmp/snmptt.ini` ファイルに追加します。その後、デーモンモードで起動している場合は `snmptt` を再起動します。

Nagiosに必要な設定ファイルをすべて追加して編集したら、次のコマンドを使用してNagiosをデバッグモードで実行します。

```
# nagios -v <NAGIOS_ETC_DIR>/nagios.cfg
```

このコマンドを受け取ると、Nagiosは設定エラーをチェックします。エラーがなかった場合は、Nagiosを通常どおりに再起動できます(たとえば、`service nagios restart` コマンドを使用して)。



Nagiosの公式マニュアルについては、<https://www.nagios.org/documentation/>を参照してください。

Dr.Web SNMP MIB

SNMPプロトコルを介して外部モニタリングシステムから取得できるDr.Web for UNIX Internet Gatewaysの動作パラメータの一覧を以下の表に示します。

パラメータ名	パラメータのOID	パラメータのタイプと説明
すべての名前に共通のプレフィックス: .iso.org.dod.internet.private.enterprises.drweb.drwebSnmpd		
すべてのOIDに共通のプレフィックス: .1.3.6.1.4.1.29690.2		
alert	イベントに関する非同期通知 (SNMPトラップ)	
threatAlert	.1.1	脅威の検出に関する通知
<i>threatAlertFile</i>	.1.1.1	感染ファイル名 (文字列)
<i>threatAlertType</i>	.1.1.2	脅威の種類 (整数*)
<i>threatAlertName</i>	.1.1.3	脅威名 (文字列)
<i>threatAlertOrigin</i>	.1.1.4	脅威を検出したコンポーネントの識別子 (整数***)
<i>threatAlertRemoteIp</i>	.1.1.5	ファイルへのアクセスに使用されたりリモートホストのIPアドレス (文字列)
<i>threatAlertRemoteUser</i>	.1.1.6	ファイルにアクセスしたりリモートユーザーの名前 (文字列)
<i>threatAlertRemoteDomain</i>	.1.1.7	ファイルへのアクセスに使用されたりリモートホストの名前 (文字列)
threatActionErrorAlert	.1.2	脅威を駆除しようとしたときに発生したエラーに関する通知
<i>threatActionErrorAlertFile</i>	.1.2.1	感染ファイル名 (文字列)
<i>threatActionErrorAlertType</i>	.1.2.2	脅威の種類 (整数*)
<i>threatActionErrorAlertName</i>	.1.2.3	脅威名 (文字列)
<i>threatActionErrorAlertOrigin</i>	.1.2.4	脅威を検出したコンポーネントの識別子 (整数***)
<i>threatActionErrorAlertError</i>	.1.2.5	エラーの説明 (文字列)
<i>threatActionErrorAlertErrorCode</i>	.1.2.6	エラーコード (エラーカタログのコードに対応する整数)



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>threatActionErrorAlertAction</i>	.1.2.7	失敗したアクション(1 - 修復、2 - 隔離へ移動、3 - 削除、4 - 報告、5 - 無視)
<i>componentFailureAlert</i>	.1.3	コンポーネント障害に関する通知
<i>componentFailureAlertName</i>	.1.3.1	コンポーネント識別子(整数***)
<i>componentFailureAlertExitCodeDescription</i>	.1.3.2	コンポーネント終了コードの説明(文字列)
<i>componentFailureAlertExitCode</i>	.1.3.3	エラーコード(エラーカタログのコードに対応する整数)
<i>infectedUrlAlert</i>	.1.4	悪質なURLのブロックに関する通知(HTTP/HTTPS接続)
<i>infectedUrlAlertUrl</i>	.1.4.1	ブロックされたURL(文字列)
<i>infectedUrlAlertDirection</i>	.1.4.2	HTTPメッセージの方向(整数:1 - 要求、2 - 応答)
<i>infectedUrlAlertType</i>	.1.4.3	脅威の種類(整数*)
<i>infectedUrlAlertName</i>	.1.4.4	脅威名(文字列)
<i>infectedUrlAlertOrigin</i>	.1.4.5	脅威を検出したコンポーネントの識別子(整数***)
<i>infectedUrlAlertSrcIp</i>	.1.4.6	接続元のIPアドレス(文字列)
<i>infectedUrlAlertSrcPort</i>	.1.4.7	接続元のポート(整数)
<i>infectedUrlAlertDstIp</i>	.1.4.8	接続先のIPアドレス(文字列)
<i>infectedUrlAlertDstPort</i>	.1.4.9	接続先のポート(整数)
<i>infectedUrlAlertSniHost</i>	.1.4.10	接続先のSNI(SSL接続)(文字列)
<i>infectedUrlAlertExePath</i>	.1.4.11	接続を確立したプログラムの実行パス(文字列)
<i>infectedUrlAlertUserName</i>	.1.4.12	接続を確立するプログラムを実行する権限を持つユーザーの名前(文字列)
<i>infectedEmailAttachmentAlert</i>	.1.5	感染したメールの添付ファイルの検出に関する通知
<i>infectedEmailAttachmentAlertType</i>	.1.5.1	脅威の種類(整数*)
<i>infectedEmailAttachmentAlertName</i>	.1.5.2	脅威名(文字列)



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>infectedEmailAttachmentAlertOrigin</i>	.1.5.3	脅威を検出したコンポーネントの識別子(整数***)
<i>infectedEmailAttachmentAlertSocket</i>	.1.5.4	メールメッセージの送信元のIPアドレス(文字列)
<i>infectedEmailAttachmentAlertMailFrom</i>	.1.5.5	メールメッセージの送信者(文字列)
<i>infectedEmailAttachmentAlertRcptTo</i>	.1.5.6	メールメッセージの受信者(文字列)
<i>infectedEmailAttachmentAlertMessageId</i>	.1.5.7	メールメッセージのMessage-IDヘッダーの値(文字列)
<i>infectedEmailAttachmentAlertAction</i>	.1.5.8	メールメッセージ全体または感染した添付ファイルに適用されたアクション(整数:1-再圧縮、2-拒否、3-破棄、4-修復、5-隔離へ移動、6-削除)
<i>infectedEmailAttachmentAlertDivert</i>	.1.5.9	メールメッセージの方向(整数:1-受信、2-送信)
<i>infectedEmailAttachmentAlertSrcIp</i>	.1.5.10	接続元のIPアドレス(文字列)
<i>infectedEmailAttachmentAlertSrcPort</i>	.1.5.11	接続元のポート(整数)
<i>infectedEmailAttachmentAlertDstIp</i>	.1.5.12	接続先のIPアドレス(文字列)
<i>infectedEmailAttachmentAlertDstPort</i>	.1.5.13	接続先のポート(整数)
<i>infectedEmailAttachmentAlertSniHost</i>	.1.5.14	接続先のSNI(SSL接続)(文字列)
<i>infectedEmailAttachmentAlertProtocol</i>	.1.5.15	プロトコルの種類(整数:1-SMTP、2-POP3、3-IMAP、4-HTTP)
<i>infectedEmailAttachmentAlertExePath</i>	.1.5.16	接続を確立したプログラムの実行パス(文字列)
<i>infectedEmailAttachmentAlertUserName</i>	.1.5.17	接続を確立するプログラムを実行する権限を持つユーザーの名前(文字列)
<i>categoryUrlAlert</i>	.1.6	不要なカテゴリーに属するURLのブロックに関する通知
<i>categoryUrlAlertUrl</i>	.1.6.1	ブロックされたURL(文字列)
<i>categoryUrlAlertCategory</i>	.1.6.2	URLが属するWebリソースカテゴリー(整数**)



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>categoryUrlAlertOrigin</i>	.1.6.3	脅威を検出したコンポーネントの識別子(整数***)
<i>categoryUrlAlertSrcIp</i>	.1.6.4	接続元のIPアドレス(文字列)
<i>categoryUrlAlertSrcPort</i>	.1.6.5	接続元のポート(整数)
<i>categoryUrlAlertDstIp</i>	.1.6.6	接続先のIPアドレス(文字列)
<i>categoryUrlAlertDstPort</i>	.1.6.7	接続先のポート(整数)
<i>categoryUrlAlertSniHost</i>	.1.6.8	接続先のSNI(SSL接続)(文字列)
<i>categoryUrlAlertExePath</i>	.1.6.9	接続を確立したプログラムの実行パス(文字列)
<i>categoryUrlAlertUserName</i>	.1.6.10	接続を確立するプログラムを実行する権限を持つユーザーの名前(文字列)
<i>categoryUrlEmailAttachmentAlert</i>	.1.7	メールメッセージ内の不要なURLの検出に関する通知
<i>categoryUrlEmailAttachmentAlertType</i>	.1.7.1	URLが属するWebリソースカテゴリ(整数**)
<i>categoryUrlEmailAttachmentAlertOrigin</i>	.1.7.2	脅威を検出したコンポーネントの識別子(整数***)
<i>categoryUrlEmailAttachmentAlertSocket</i>	.1.7.3	メールメッセージの送信元のIPアドレス(文字列)
<i>categoryUrlEmailAttachmentAlertMailFrom</i>	.1.7.4	メールメッセージの送信者(文字列)
<i>categoryUrlEmailAttachmentAlertRcptTo</i>	.1.7.5	メールメッセージの受信者(文字列)
<i>categoryUrlEmailAttachmentAlertMessageId</i>	.1.7.6	メールメッセージのMessage-IDヘッダーの値(文字列)
<i>categoryUrlEmailAttachmentAlertAction</i>	.1.7.7	メールメッセージ全体または添付ファイルに適用されたアクション(整数:1-再圧縮、2-拒否、3-破棄、4-修復、5-隔離へ移動、6-削除)
<i>categoryUrlEmailAttachmentAlertDivert</i>	.1.7.8	メールメッセージの方向(整数:1-受信、2-送信)
<i>categoryUrlEmailAttachmentAlertSrcIp</i>	.1.7.9	接続元のIPアドレス(文字列)



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>categoryUrlEmailAttachmentAlertSrcPort</i>	.1.7.10	接続元のポート(整数)
<i>categoryUrlEmailAttachmentAlertDstIp</i>	.1.7.11	接続先のIPアドレス(文字列)
<i>categoryUrlEmailAttachmentAlertDstPort</i>	.1.7.12	接続先のポート(整数)
<i>categoryUrlEmailAttachmentAlertSniHost</i>	.1.7.13	接続先のSNI(SSL接続)(文字列)
<i>categoryUrlEmailAttachmentAlertProtocol</i>	.1.7.14	プロトコルの種類(整数: 1 - SMTP、2 - POP3、3 - IMAP、4 - HTTP)
<i>categoryUrlEmailAttachmentAlertExePath</i>	.1.7.15	接続を確立したプログラムの実行パス(文字列)
<i>categoryUrlEmailAttachmentAlertUserName</i>	.1.7.16	接続を確立するプログラムを実行する権限を持つユーザーの名前(文字列)
spamEmailAlert	.1.8	メールメッセージのスパム認識に関する通知
<i>spamEmailAlertOrigin</i>	.1.8.1	脅威を検出したコンポーネントの識別子(整数 ***)
<i>spamEmailAlertSocket</i>	.1.8.2	メールメッセージの送信元のIPアドレス(文字列)
<i>spamEmailAlertMailFrom</i>	.1.8.3	メールメッセージの送信者(文字列)
<i>spamEmailAlertRcptTo</i>	.1.8.4	メールメッセージの受信者(文字列)
<i>spamEmailAlertMessageId</i>	.1.8.5	メールメッセージのMessage-IDヘッダーの値(文字列)
<i>spamEmailAlertAction</i>	.1.8.6	メールメッセージ全体または添付ファイルに適用されたアクション(整数: 1 - 再圧縮、2 - 拒否、3 - 破棄、4 - 修復、5 - 隔離へ移動、6 - 削除)
<i>spamEmailAlertDivert</i>	.1.8.7	メールメッセージの方向(整数: 1 - 受信、2 - 送信)
<i>spamEmailAlertSrcIp</i>	.1.8.8	接続元のIPアドレス(文字列)
<i>spamEmailAlertSrcPort</i>	.1.8.9	接続元のポート(整数)
<i>spamEmailAlertDstIp</i>	.1.8.10	接続先のIPアドレス(文字列)



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>spamEmailAlertDstPort</i>	.1.8.11	接続先のポート(整数)
<i>spamEmailAlertSniHost</i>	.1.8.12	接続先のSNI(SSL接続)(文字列)
<i>spamEmailAlertProtocol</i>	.1.8.13	プロトコルの種類(整数:1 - SMTP、2 - POP3、3 - IMAP、4 - HTTP)
<i>spamEmailAlertExePath</i>	.1.8.14	接続を確立したプログラムの実行パス(文字列)
<i>spamEmailAlertUserName</i>	.1.8.15	接続を確立するプログラムを実行する権限を持つユーザーの名前(文字列)
<i>blockedConnectionAlert</i>	.1.9	ネットワーク接続のブロックに関する通知
<i>blockedConnectionAlertOrigin</i>	.1.9.1	脅威を検出したコンポーネントの識別子(整数***)
<i>blockedConnectionAlertDivert</i>	.1.9.2	接続の方向(整数:1 - 受信、2 - 送信)
<i>blockedConnectionAlertSrcIp</i>	.1.9.3	接続元のIPアドレス(文字列)
<i>blockedConnectionAlertSrcPort</i>	.1.9.4	接続元のポート(整数)
<i>blockedConnectionAlertDstIp</i>	.1.9.5	接続先のIPアドレス(文字列)
<i>blockedConnectionAlertDstPort</i>	.1.9.6	接続先のポート(整数)
<i>blockedConnectionAlertSniHost</i>	.1.9.7	接続先のSNI(SSL接続)(文字列)
<i>blockedConnectionAlertProtocol</i>	.1.9.8	プロトコルの種類(整数:1 - SMTP、2 - POP3、3 - IMAP、4 - HTTP)
<i>blockedConnectionAlertExePath</i>	.1.9.9	接続を確立したプログラムの実行パス(文字列)
<i>blockedConnectionAlertUserName</i>	.1.9.10	接続を確立するプログラムを実行する権限を持つユーザーの名前(文字列)
stat	Dr.Web for UNIX Internet Gatewaysの動作に関する統計	
<i>threatCounters</i>	.2.1	検出された脅威のカウンター



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>knownVirus</i>	.2.1.1	検出された既知のウイルスの数(カウンター、整数)
<i>suspicious</i>	.2.1.2	検出された疑わしいオブジェクトの数(カウンター、整数)
<i>adware</i>	.2.1.3	検出されたアドウェアの数(カウンター、整数)
<i>dialers</i>	.2.1.4	検出されたダイヤラーの数(カウンター、整数)
<i>joke</i>	.2.1.5	検出されたジョークプログラムの数(カウンター、整数)
<i>riskware</i>	.2.1.6	検出されたリスクウェアの数(カウンター、整数)
<i>hacktool</i>	.2.1.7	検出されたハッキングツールの数(カウンター、整数)
scanErrors	.2.2	ファイルのスキャン中に発生したエラーのカウンター
<i>sePathNotAbsolute</i>	.2.2.1	「パスが絶対パスではありません」エラーの発生回数(カウンター、整数)
<i>seFileNotFound</i>	.2.2.2	「ファイルが見つかりません」エラーの発生回数(カウンター、整数)
<i>seFileNotRegular</i>	.2.2.3	「ファイルは通常のファイルではありません」エラーの発生回数(カウンター、整数)
<i>seFileNotBlockDevice</i>	.2.2.4	「ファイルはブロックデバイスではありません」エラーの発生回数(カウンター、整数)
<i>seNameTooLong</i>	.2.2.5	「パスまたはファイル名が長すぎます」エラーの発生回数(カウンター、整数)
<i>seNoAccess</i>	.2.2.6	「パーミッションが拒否されました」エラーの発生回数(カウンター、整数)
<i>seReadError</i>	.2.2.7	「読み取りエラー」の発生回数(カウンター、整数)
<i>seWriteError</i>	.2.2.8	「書き込みエラー」の発生回数(カウンター、整数)



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>seFileTooLarge</i>	.2.2.9	「ファイルサイズが大きすぎます」エラーの発生回数(カウンター、整数)
<i>seFileBusy</i>	.2.2.10	「ファイルがビジーです」エラーの発生回数(カウンター、整数)
<i>seUnpackingError</i>	.2.2.20	「アンパックエラー」の発生回数(カウンター、整数)
<i>sePasswordProtectetd</i>	.2.2.21	「パスワード保護」エラーの発生回数(カウンター、整数)
<i>seArchCrcError</i>	.2.2.22	「アーカイブのCRCエラー」の発生回数(カウンター、整数)
<i>seArchInvalidHeader</i>	.2.2.23	「無効なアーカイブヘッダーです」エラーの発生回数(カウンター、整数)
<i>seArchNoMemory</i>	.2.2.24	「アーカイブを処理するのに十分なメモリがありません」エラーの発生回数(カウンター、整数)
<i>seArchIncomplete</i>	.2.2.25	「不完全なアーカイブ」エラーの発生回数(カウンター、整数)
<i>seCanNotBeCured</i>	.2.2.26	「オブジェクトを修復できません」エラーの発生回数(カウンター、整数)
<i>sePackerLevelLimit</i>	.2.2.30	「圧縮されたオブジェクトが最大ネスティングレベルを超えました」エラーの発生回数(カウンター、整数)
<i>seArchiveLevelLimit</i>	.2.2.31	「アーカイブが最大ネスティングレベルを超えました」エラーの発生回数(カウンター、整数)
<i>seMailLevelLimit</i>	.2.2.32	「メールファイルが最大ネスティングレベルを超えました」エラーの発生回数(カウンター、整数)
<i>seContainerLevelLimit</i>	.2.2.33	「コンテナファイルが最大ネスティングレベルを超えました」エラーの発生回数(カウンター、整数)
<i>seCompressionLimit</i>	.2.2.34	「最大圧縮率を超えました」エラーの発生回数(カウンター、整数)
<i>seReportSizeLimit</i>	.2.2.35	「スキャン結果レポートの最大サイズを超えました」エラーの発生回数(カウンター、整数)



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>seScanTimeout</i>	.2.2.40	「スキャンタイムアウトに達しました」エラーの発生回数(カウンター、整数)
<i>seEngineCrash</i>	.2.2.41	「Scan Engineのクラッシュが検出されました」エラーの発生回数(カウンター、整数)
<i>seEngineHangup</i>	.2.2.42	「Scan Engineが応答を停止しました」エラーの発生回数(カウンター、整数)
<i>seEngineError</i>	.2.2.44	「Scan Engineの内部エラー」の発生回数(カウンター、整数)
<i>seNoLicense</i>	.2.2.45	「有効なライセンスが見つかりません」エラーの発生回数(カウンター、整数)
<i>seCuringLimitReached</i>	.2.2.47	「修復試行限界に達しました」エラーの発生数(カウンター、整数)
<i>seNonSupportedDisk</i>	.2.2.50	「サポートされていないディスクです」エラーの発生回数(カウンター、整数)
<i>seUnexpectedError</i>	.2.2.100	「予期せぬエラーです」の発生数(カウンター、整数)
scanLoadAverage	.2.3	ファイルスキャン負荷の指標
<i>filesScannedTable</i>	.2.3.1	他のコンポーネントのリクエストによりスキャンされたファイルの平均数
filesScannedEntry	.2.3.1.1	製品のコンポーネント(テーブル行全体、レコード)
filesScannedIndex	.2.3.1.1.1	コンポーネントのインデックス(識別子、整数***)
filesScannedOrigin	.2.3.1.1.2	コンポーネントの名前
filesScanned1min	.2.3.1.1.3	1秒間にチェックされたファイルの平均(1分間の平均)数(文字列)
filesScanned5min	.2.3.1.1.4	1秒間にチェックされたファイルの平均(5分間の平均)数(文字列)
filesScanned15min	.2.3.1.1.5	1秒間にチェックされたファイルの平均(15分間の平均)数(文字列)
<i>bytesScannedTable</i>	.2.3.2	他のコンポーネントのリクエストにより実行されたスキャンの平均速度



パラメータ名	パラメータのOID	パラメータのタイプと説明
		(1秒あたりのバイト数)
bytesScannedEntry	.2.3.2.1	製品のコンポーネント(テーブル行全体、レコード)
bytesScannedIndex	.2.3.2.1.1	コンポーネントのインデックス(識別子、整数***)
bytesScannedOrigin	.2.3.2.1.2	コンポーネントの名前
bytesScanned1min	.2.3.2.1.3	1秒間にスキャンされた平均バイト数(1分間の平均)(文字列)
bytesScanned5min	.2.3.2.1.4	1秒間にスキャンされた平均バイト数(5分間の平均)(文字列)
bytesScanned15min	.2.3.2.1.5	1秒間にスキャンされた平均バイト数(15分間の平均)(文字列)
<i>cacheHitFilesTable</i>	.2.3.3	コンポーネントのリクエストによりキャッシュから取得されたスキャンレポートの平均数
cacheHitFilesEntry	.2.3.3.1	製品のコンポーネント(テーブル行全体、レコード)
cacheHitFilesIndex	.2.3.3.1.1	コンポーネントのインデックス(識別子、整数***)
cacheHitFilesOrigin	.2.3.3.1.2	コンポーネントの名前
cacheHitFiles1min	.2.3.3.1.3	1秒間にキャッシュから取得されたレポートの平均(1分間の平均)数(文字列)
cacheHitFiles5min	.2.3.3.1.4	1秒間にキャッシュから取得されたレポートの平均(5分間の平均)数(文字列)
cacheHitFiles15min	.2.3.3.1.5	1秒間にキャッシュから取得されたレポートの平均(15分間の平均)数(文字列)
<i>errorsTable</i>	.2.3.4	コンポーネントのリクエストにより実行されたスキャン中の平均エラー数
errorsEntry	.2.3.4.1	製品のコンポーネント(テーブル行全体、レコード)
errorsIndex	.2.3.4.1.1	コンポーネントのインデックス(識別子、整数***)
errorsOrigin	.2.3.4.1.2	コンポーネントの名前



パラメータ名	パラメータのOID	パラメータのタイプと説明
errors1min	.2.3.4.1.3	1秒間のスキャンエラーの平均(1分間の平均)数(文字列)
errors5min	.2.3.4.1.4	1秒間のスキャンエラーの平均(5分間の平均)数(文字列)
errors15min	.2.3.4.1.5	1秒間のスキャンエラーの平均(15分間の平均)数(文字列)
net	.2.4	ネットワークアクティビティの統計
markedAsSpam	.2.4.1	スパムとしてマークされたメールメッセージの数(カウンター、整数)
blockedInfectionSource	.2.4.101	「感染源」カテゴリーに属するブロックされたURLの数(カウンター、整数)
blockedNotRecommended	.2.4.102	「非推奨」カテゴリーに属するブロックされたURLの数(カウンター、整数)
blockedAdultContent	.2.4.103	「アダルトコンテンツ」カテゴリーに属するブロックされたURLの数(カウンター、整数)
blockedViolence	.2.4.104	「暴力」カテゴリーに属するブロックされたURLの数(カウンター、整数)
blockedWeapons	.2.4.105	「武器」カテゴリーに属するブロックされたURLの数(カウンター、整数)
blockedGambling	.2.4.106	「ギャンブル」カテゴリーに属するブロックされたURLの数(カウンター、整数)
blockedDrugs	.2.4.107	「麻薬」カテゴリーに属するブロックされたURLの数(カウンター、整数)
blockedObsceneLanguage	.2.4.108	「卑猥な表現」カテゴリーに属するブロックされたURLの数(カウンター、整数)
blockedChats	.2.4.109	「チャット」カテゴリーに属するブロックされたURLの数(カウンター、整数)
blockedTerrorism	.2.4.110	「テロリズム」カテゴリーに属するブロックされたURLの数(カウンター、整数)
blockedFreeEmail	.2.4.111	「無料メールサービス」カテゴリーに属するブロックされたURLの数(カウ



パラメータ名	パラメータのOID	パラメータのタイプと説明
		ンター、整数)
<i>blockedSocialNetworks</i>	.2.4.112	「ソーシャルネットワーク」カテゴリに属するブロックされたURLの数(カウンター、整数)
<i>blockedOwnersNotice</i>	.2.4.113	「著作権者の申し立て」カテゴリに属するブロックされたURLの数(カウンター、整数)
<i>blockedOnlineGames</i>	.2.4.114	「オンラインゲーム」カテゴリに属するブロックされたURLの数(カウンター、整数)
<i>blockedAnonymizers</i>	.2.4.115	「アノニマイザー」カテゴリに属するブロックされたURLの数(カウンター、整数)
<i>blockedCryptocurrencyMiningPools</i>	.2.4.116	「仮想通貨マイニングプール」カテゴリに属するブロックされたURLの数(カウンター、整数)
<i>blockedJobs</i>	.2.4.117	「求人情報サイト」カテゴリに属するブロックされたURLの数(カウンター、整数)
<i>blockedBlackList</i>	.2.4.120	ユーザーのブラックリストからブロックされたURLの数(カウンター、整数)
info	Dr.Web for UNIX Internet Gatewaysの現在の状態に関する情報	
components	.3.1	Dr.Web for UNIX Internet Gatewaysコンポーネントのステータス
<i>configd</i>	.3.1.1	drweb-configdコンポーネントデータ
configdState	.3.1.1.1	コンポーネントの現在の状態(整数****)
configdExitCode	.3.1.1.2	前回の終了コード(エラーカタログのコードに対応する整数)
configdExitTime	.3.1.1.3	前回の終了時刻(<i>UNIX時間</i>)
configdInstalledApps	.3.1.1.101	インストールされているコンポーネントのリスト
configdAppEntry	.3.1.1.101.1	インストールされているコンポーネントに関する情報(テーブル行全体、レコード)



パラメータ名	パラメータのOID	パラメータのタイプと説明
configAppIndex	.3.1.1.101.1.1	インストールされているコンポーネントのインデックス(序数)(整数)
configAppName	.3.1.1.101.1.2	インストールされているコンポーネントの名前(文字列)
configAppExePath	.3.1.1.101.1.3	コンポーネントの実行パス(文字列)
configAppInstallTime	.3.1.1.101.1.4	コンポーネントがインストールされた時刻(<i>UNIX時間</i>)
configAppIniSection	.3.1.1.101.1.5	設定ファイルにあるコンポーネントのパラメータを含むセクションの名前
<i>scanEngine</i>	.3.1.2	drweb-seコンポーネントデータ
scanEngineState	.3.1.2.1	コンポーネントの現在の状態(整数****)
scanEngineExitCode	.3.1.2.2	前回の終了コード(エラーカタログのコードに対応する整数)
scanEngineExitTime	.3.1.2.3	前回の終了時刻(<i>UNIX時間</i>)
scanEngineStatus	.3.1.2.101	Dr.Web Virus-Finding Engineの現在の状態(整数)
scanEngineVersion	.3.1.2.102	Dr.Web Virus-Finding Engineのバージョン(文字列)
scanEngineVirusRecords	.3.1.2.103	ウイルスレコードの数(整数)
scanEngineMaxForks	.3.1.2.104	スキャン対象の子プロセスの最大数(整数)
scanEngineQueues	.3.1.2.105	スキャンタスクのキュー
scanEngineQueuesLow	.3.1.2.105.1	優先度の低いタスクのキュー
scanEngineQueueLowOut	.3.1.2.105.1.1	キューから出て処理に転送された優先度の低いタスクの数(カウンター、整数)
scanEngineQueueLowSize	.3.1.2.105.1.2	キュー内で処理待ちになっている優先度の低いタスクの数(カウンター、整数)
scanEngineQueuesMedium	.3.1.2.105.2	通常優先度のタスクのキュー
scanEngineQueueMediumOut	.3.1.2.105.2.1	キューから出て処理に転送された通常優先度のタスクの数(カウンター、整数)



パラメータ名	パラメータのOID	パラメータのタイプと説明
scanEngineQueueMediumSize	.3.1.2.105.2.2	キュー内で処理待ちになっている通常優先度のタスクの数(カウンター、整数)
scanEngineQueuesHigh	.3.1.2.105.3	優先度の高いタスクのキュー
scanEngineQueueHighOut	.3.1.2.105.3.1	キューから出て処理に転送された優先度の高いタスクの数(カウンター、整数)
scanEngineQueueHighSize	.3.1.2.105.3.2	キュー内で処理待ちになっている優先度の高いタスクの数(カウンター、整数)
scanEngineVirusBasesTable	.3.1.2.106	ウイルスデータベースのリスト
scanEngineVirusBasesEntry	.3.1.2.106.1	ウイルスデータベースに関する情報(テーブル行全体、レコード)
scanEngineVirusBaseIndex	.3.1.2.106.1.1	ウイルスデータベースのインデックス(整数)
scanEngineVirusBasePath	.3.1.2.106.1.2	ウイルスデータベースファイルへのパス(文字列)
scanEngineVirusBaseRecords	.3.1.2.106.1.3	ウイルスデータベース内のレコード数(整数)
scanEngineVirusBaseVersion	.3.1.2.106.1.4	ウイルスデータベースのバージョン(整数)
scanEngineVirusBaseTimestamp	.3.1.2.106.1.5	ウイルスデータベースのタイムスタンプ(<i>UNIX時間</i>)
scanEngineVirusBaseMD5	.3.1.2.106.1.6	MD5チェックサム(文字列)
scanEngineVirusBaseLoadResult	.3.1.2.106.1.7	このウイルスデータベースのダウンロード結果(文字列)
scanEngineQueuesTab	.3.1.2.107	スキャンタスクキューのリスト
scanEngineQueueEntry	.3.1.2.107.1	キューに関する情報(テーブル行全体、レコード)
scanEngineQueueIndex	.3.1.2.107.1.1	キューのインデックス(序数)(整数)
scanEngineQueueName	.3.1.2.107.1.2	キューの名前(文字列)
scanEngineQueueOut	.3.1.2.107.1.3	キューから出て処理に転送されたタスクの数(カウンター、整数)



パラメータ名	パラメータのOID	パラメータのタイプと説明
scanEngineQueueSize	.3.1.2.107.1.4	キュー内で処理待ちになっているタスクの数(カウンター、整数)
<i>fileCheck</i>	.3.1.3	drweb-filecheckコンポーネントデータ
fileCheckState	.3.1.3.1	コンポーネントの現在の状態(整数****)
fileCheckExitCode	.3.1.3.2	前回の終了コード(エラーカタログのコードに対応する整数)
fileCheckExitTime	.3.1.3.3	前回の終了時刻(<i>UNIX時間</i>)
fileCheckScannedFiles	.3.1.3.101	スキャン済みファイル数(カウンター、整数)
fileCheckScannedBytes	.3.1.3.102	スキャン済みバイト数(カウンター、整数)
fileCheckCacheHitFiles	.3.1.3.103	キャッシュから取得したスキャンレポートの数(カウンター、整数)
fileCheckScanErrors	.3.1.3.104	スキャンエンジンでのエラーの発生回数(カウンター、整数)
fileCheckScanStat	.3.1.3.105	クライアントのリスト
fileCheckClientEntry	.3.1.3.105.1	クライアントに関する情報(テーブル行全体、レコード)
fileCheckClientIndex	.3.1.3.105.1.1	クライアントのインデックス(序数)(整数)
fileCheckClientName	.3.1.3.105.1.2	クライアントコンポーネントの名前(文字列)
fileCheckClientScannedFiles	.3.1.3.105.1.3	このクライアントでスキャンされたファイル数(カウンター、整数)
fileCheckClientScannedBytes	.3.1.3.105.1.4	このクライアントでスキャンされたバイト数(カウンター、整数)
fileCheckClientCacheHitFiles	.3.1.3.105.1.5	このクライアントのキャッシュから取得したスキャンレポートの数(カウンター、整数)
fileCheckClientScanErrors	.3.1.3.105.1.6	このクライアントで動作しているときにスキャンエンジンで発生したエラーの数(カウンター、整数)
<i>update</i>	.3.1.4	drweb-updateコンポーネントデータ



パラメータ名	パラメータのOID	パラメータのタイプと説明
updateState	.3.1.4.1	コンポーネントの現在の状態(整数****)
updateExitCode	.3.1.4.2	前回の終了コード(エラーカタログのコードに対応する整数)
updateExitTime	.3.1.4.3	前回の終了時刻(<i>UNIX時間</i>)
updateBytesSent	.3.1.4.101	送信したバイト数(カウンター、整数)
updateBytesReceived	.3.1.4.102	受信したバイト数(カウンター、整数)
<i>esagent</i>	.3.1.5	drweb-esagentコンポーネントデータ
esagentState	.3.1.5.1	コンポーネントの現在の状態(整数****)
esagentExitCode	.3.1.5.2	前回の終了コード(エラーカタログのコードに対応する整数)
esagentExitTime	.3.1.5.3	前回の終了時刻(<i>UNIX時間</i>)
esagentWorkStatus	.3.1.5.101	コンポーネントの現在の動作モード(整数: 1 - スタンドアロンモード、2 - 接続中、3 - 接続待ち、4 - 接続承認済み)
esagentIsConnected	.3.1.5.102	サーバーに接続されているかどうか(整数、0 - いいえ、1 - はい)
esagentServer	.3.1.5.103	使用されている集中管理サーバーのアドレス(文字列)
<i>netcheck</i>	.3.1.6	drweb-netcheckコンポーネントデータ
netcheckState	.3.1.6.1	コンポーネントの現在の状態(整数****)
netcheckExitCode	.3.1.6.2	前回の終了コード(エラーカタログのコードに対応する整数)
netcheckExitTime	.3.1.6.3	前回の終了時刻(<i>UNIX時間</i>)
netcheckLocalSeForks	.3.1.6.101	ローカルで利用可能なスキャンエンジンプロセスの数(整数)
netcheckRemoteSeForks	.3.1.6.102	リモートで利用可能なスキャンエンジンプロセスの数(整数)



パラメータ名	パラメータのOID	パラメータのタイプと説明
netcheckLocalFilesScanned	.3.1.6.103	ローカルでスキャンされたファイルの数(カウンター、整数)
netcheckNetworkFilesScanned	.3.1.6.104	リモートスキャンでスキャンされたファイルの数(カウンター、整数)
netcheckLocalBytesScanned	.3.1.6.105	ローカルでスキャンされたバイト数(カウンター、整数)
netcheckNetworkBytesScanned	.3.1.6.106	リモートスキャンでスキャンされたバイト数(カウンター、整数)
netcheckLocalBytesIn	.3.1.6.107	ローカルクライアントから受信したバイト数(カウンター、整数)
netcheckLocalBytesOut	.3.1.6.108	ローカルクライアントに送信したバイト数(カウンター、整数)
netcheckNetworkBytesIn	.3.1.6.109	リモートホストから受信したバイト数(カウンター、整数)
netcheckNetworkBytesOut	.3.1.6.110	リモートホストに送信したバイト数(カウンター、整数)
netcheckLocalScanErrors	.3.1.6.111	ローカルのスキャンエンジンプロセスでのエラーの発生回数(カウンター、整数)
netcheckNetworkScanErrors	.3.1.6.112	リモートのスキャンエンジンプロセスでのエラーの発生回数(カウンター、整数)
<i>httpd</i>	.3.1.7	drweb-httpdコンポーネントデータ
httpdState	.3.1.7.1	コンポーネントの現在の状態(整数****)
httpdExitCode	.3.1.7.2	前回の終了コード(エラーカタログのコードに対応する整数)
httpdExitTime	.3.1.7.3	前回の終了時刻(<i>UNIX時間</i>)
<i>snmpd</i>	.3.1.8	drweb-snmpdコンポーネントデータ
snmpdState	.3.1.8.1	コンポーネントの現在の状態(整数****)
snmpdExitCode	.3.1.8.2	前回の終了コード(エラーカタログのコードに対応する整数)
snmpdExitTime	.3.1.8.3	前回の終了時刻(<i>UNIX時間</i>)



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>clamd</i>	.3.1.20	drweb-clamdコンポーネントデータ
clamdState	.3.1.20.1	コンポーネントの現在の状態(整数****)
clamdExitCode	.3.1.20.2	前回の終了コード(エラーカタログのコードに対応する整数)
clamdExitTime	.3.1.20.3	前回の終了時刻(<i>UNIX時間</i>)
<i>icapd</i>	.3.1.21	drweb-icapdコンポーネントデータ
icapdState	.3.1.21.1	コンポーネントの現在の状態(整数****)
icapdExitCode	.3.1.21.2	前回の終了コード(エラーカタログのコードに対応する整数)
icapdExitTime	.3.1.21.3	前回の終了時刻(<i>UNIX時間</i>)
icapdConnectionsIn	.3.1.21.101	承認された受信接続の数(カウンター、整数)
icapdConnectionsCount	.3.1.21.102	現在開いている接続の数(カウンター、整数)
icapdOptions	.3.1.21.103	<i>OPTIONS</i> リクエストの数(カウンター、整数)
icapdReqmod	.3.1.21.104	<i>REQMOD</i> リクエストの数(カウンター、整数)
icapdRespmo	.3.1.21.105	<i>RESPMOD</i> リクエストの数(カウンター、整数)
icapdBad	.3.1.21.106	無効なリクエストの数(カウンター、整数)
<i>smbspider</i>	.3.1.40	drweb-smbspider-daemonコンポーネントデータ
smbspiderState	.3.1.40.1	コンポーネントの現在の状態(整数****)
smbspiderExitCode	.3.1.40.2	前回の終了コード(エラーカタログのコードに対応する整数)
smbspiderExitTime	.3.1.40.3	前回の終了時刻(<i>UNIX時間</i>)



パラメータ名	パラメータのOID	パラメータのタイプと説明
smbspiderConnectionsIn	.3.1.40.101	開かれた接続の合計数(カウンター、整数)
smbspiderConnectionsCount	.3.1.40.102	現在開いている接続の数(カウンター、整数)
smbspiderShareTable	.3.1.40.103	保護されたSamba共有リソースに関する統計
smbspiderShareEntry	.3.1.40.103.1	保護されているSamba共有リソースに関する情報(テーブル行全体、レコード)
smbspiderShareIndex	.3.1.40.103.1.1	保護されたSamba共有リソースのインデックス(序数)(整数)
smbspiderSharePath	.3.1.40.103.1.2	保護されたSamba共有リソースへのパス(文字列)
smbspiderShareConnectionsIn	.3.1.40.103.1.3	開かれた接続の合計数(カウンター、整数)
smbspiderShareConnectionsCount	.3.1.40.103.1.4	現在開いている接続の数(カウンター、整数)
<i>gated</i>	.3.1.41	drweb-gatedコンポーネントデータ
gatedState	.3.1.41.1	コンポーネントの現在の状態(整数****)
gatedExitCode	.3.1.41.2	前回の終了コード(エラーカタログのコードに対応する整数)
gatedExitTime	.3.1.41.3	前回の終了時刻(<i>UNIX時間</i>)
gatedInterceptedIn	.3.1.41.101	傍受した接続の数(カウンター、整数)
gatedInterceptedCount	.3.1.41.102	現在モニタリングされている接続の数(カウンター、整数)
<i>maild</i>	.3.1.42	drweb-maildコンポーネントデータ
maildState	.3.1.42.1	コンポーネントの現在の状態(整数****)
maildExitCode	.3.1.42.2	前回の終了コード(エラーカタログのコードに対応する整数)
maildExitTime	.3.1.42.3	前回の終了時刻(<i>UNIX時間</i>)



パラメータ名	パラメータのOID	パラメータのタイプと説明
maildStat	.3.1.42.4	drweb-maildコンポーネントの動作の統計
maildStatNative	.3.1.42.4.1	コンポーネントの内部インターフェースdrweb-maildを介したメールスキャンの統計(傍受したSMTP、POP3、IMAP接続のスキャン中にSpIDer Gateが受信したメッセージ)
maildStatNativePassed	.3.1.42.4.1.1	受信できなかったメッセージの数(カウンター、整数)
maildStatNativeRepacked	.3.1.42.4.1.2	再圧縮されたメッセージの数(カウンター、整数)
maildStatNativeRejected	.3.1.42.4.1.3	拒否されたメッセージの数(カウンター、整数)
maildStatNativeFailed	.3.1.42.4.1.4	メッセージスキャンエラーの数(カウンター、整数)
maildStatNativeQueueSize	.3.1.42.4.1.5	キューライン、つまりインターフェースを介したスキャンを待機しているファイルの数(整数)
maildStatMilter	.3.1.42.4.2	drweb-maildコンポーネントのコンポーネントインターフェースMilterを介したメールスキャンの統計
maildStatMilterPassed	.3.1.42.4.2.1	受信できなかったメッセージの数(カウンター、整数)
maildStatMilterRepacked	.3.1.42.4.2.2	再圧縮されたメッセージの数(カウンター、整数)
maildStatMilterRejected	.3.1.42.4.2.3	拒否されたメッセージの数(カウンター、整数)
maildStatMilterFailed	.3.1.42.4.2.4	メッセージスキャンエラーの数(カウンター、整数)
maildStatMilterQueueSize	.3.1.42.4.2.5	キューライン、つまりインターフェースを介したスキャンを待機しているファイルの数(整数)
maildStatSpamc	.3.1.42.4.3	drweb-maildコンポーネントのコンポーネントインターフェースSpamcを介したメールスキャンの統計
maildStatSpamcPassed	.3.1.42.4.3.1	受信できなかったメッセージの数(カウンター、整数)



パラメータ名	パラメータのOID	パラメータのタイプと説明
maildStatSpamcRepacked	.3.1.42.4.3.2	再圧縮されたメッセージの数(カウンター、整数)
maildStatSpamcRejected	.3.1.42.4.3.3	拒否されたメッセージの数(カウンター、整数)
maildStatSpamcFailed	.3.1.42.4.3.4	メッセージスキャンエラーの数(カウンター、整数)
maildStatSpamcQueueSize	.3.1.42.4.3.5	キューライン、つまりインターフェースを介したスキャンを待機しているファイルの数(整数)
maildStatRspamc	.3.1.42.4.4	drweb-maildコンポーネントのコンポーネントインターフェース <i>Rspamc</i> を介したメールスキャンの統計
maildStatRspamcPassed	.3.1.42.4.4.1	受信できなかったメッセージの数(カウンター、整数)
maildStatRspamcRepacked	.3.1.42.4.4.2	再圧縮されたメッセージの数(カウンター、整数)
maildStatRspamcRejected	.3.1.42.4.4.3	拒否されたメッセージの数(カウンター、整数)
maildStatRspamcFailed	.3.1.42.4.4.4	メッセージスキャンエラーの数(カウンター、整数)
maildStatRspamcQueueSize	.3.1.42.4.4.5	キューライン、つまりインターフェースを介したスキャンを待機しているファイルの数(整数)
<i>lookupd</i>	.3.1.43	drweb-lookupdコンポーネントデータ
lookupdState	.3.1.43.1	コンポーネントの現在の状態(整数****)
lookupdExitCode	.3.1.43.2	前回の終了コード(エラーカタログのコードに対応する整数)
lookupdExitTime	.3.1.43.3	前回の終了時刻(<i>UNIX時間</i>)
<i>antispam</i>	.3.1.44	drweb-aseコンポーネントに関するデータ
antispamState	.3.1.44.1	コンポーネントの現在の状態(整数****)
antispamExitCode	.3.1.44.2	前回の終了コード(エラーカタログのコードに対応する整数)



パラメータ名	パラメータのOID	パラメータのタイプと説明
antispamExitTime	.3.1.44.3	前回の終了時刻 (<i>UNIX時間</i>)
<i>cloudd</i>	.3.1.50	drweb-clouddコンポーネントデータ
clouddState	.3.1.50.1	コンポーネントの現在の状態 (整数****)
clouddExitCode	.3.1.50.2	前回の終了コード (エラーカタログのコードに対応する整数)
clouddExitTime	.3.1.50.3	前回の終了時刻 (<i>UNIX時間</i>)
<i>meshd</i>	.3.1.52	drweb-meshdコンポーネントデータ
meshdState	.3.1.52.1	コンポーネントの現在の状態 (整数****)
meshdExitCode	.3.1.52.2	前回の終了コード (エラーカタログのコードに対応する整数)
meshdExitTime	.3.1.52.3	前回の終了時刻 (<i>UNIX時間</i>)
<i>lotus</i>	.3.1.60	drweb-lotusコンポーネントデータ
lotusState	.3.1.60.1	コンポーネントの現在の状態 (整数****)
lotusExitCode	.3.1.60.2	前回の終了コード (エラーカタログのコードに対応する整数)
lotusExitTime	.3.1.60.3	前回の終了時刻 (<i>UNIX時間</i>)
<i>macgui</i>	.3.1.100	drweb-gui (macOS用)コンポーネントデータ
macguiState	.3.1.100.1	コンポーネントの現在の状態 (整数****)
macguiExitCode	.3.1.100.2	前回の終了コード (エラーカタログのコードに対応する整数)
macguiExitTime	.3.1.100.3	前回の終了時刻 (<i>UNIX時間</i>)
<i>macspider</i>	.3.1.102	drweb-spider (macOS用)コンポーネントデータ
macspiderState	.3.1.102.1	コンポーネントの現在の状態 (整数****)



パラメータ名	パラメータのOID	パラメータのタイプと説明
macspiderExitCode	.3.1.102.2	前回の終了コード(エラーカタログのコードに対応する整数)
macspiderExitTime	.3.1.102.3	前回の終了時刻(<i>UNIX時間</i>)
macspiderWorkStatus	.3.1.102.101	コンポーネントの現在の動作モード(整数:0-未設定、1-読み込み中、2-実行中)
<i>macfirewall</i>	.3.1.103	drweb-firewall(macOS用)コンポーネントデータ
macfirewallState	.3.1.103.1	コンポーネントの現在の状態(整数****)
macfirewallExitCode	.3.1.103.2	前回の終了コード(エラーカタログのコードに対応する整数)
macfirewallExitTime	.3.1.103.3	前回の終了時刻(<i>UNIX時間</i>)
<i>linuxgui</i>	.3.1.200	drweb-gui(GNU/Linux用)コンポーネントデータ
linuxguiState	.3.1.200.1	コンポーネントの現在の状態(整数****)
linuxguiExitCode	.3.1.200.2	前回の終了コード(エラーカタログのコードに対応する整数)
linuxguiExitTime	.3.1.200.3	前回の終了時刻(<i>UNIX時間</i>)
<i>linuxspider</i>	.3.1.201	drweb-spider(GNU/Linux用)コンポーネントデータ
linuxspiderState	.3.1.201.1	コンポーネントの現在の状態(整数****)
linuxspiderExitCode	.3.1.201.2	前回の終了コード(エラーカタログのコードに対応する整数)
linuxspiderExitTime	.3.1.201.3	前回の終了時刻(<i>UNIX時間</i>)
linuxspiderWorkStatus	.3.1.201.101	コンポーネントの現在の動作モード(整数:0-未設定、1-読み込み中、2-fanotify経由で実行中、3-LKM経由で実行中)
<i>linuxnss</i>	.3.1.202	drweb-nss(GNU/Linux用)コンポーネントデータ
linuxnssState	.3.1.202.1	コンポーネントの現在の状態(整数****)



パラメータ名	パラメータのOID	パラメータのタイプと説明
linuxnssExitCode	.3.1.202.2	前回の終了コード(エラーカタログのコードに対応する整数)
linuxnssExitTime	.3.1.202.3	前回の終了時刻(<i>UNIX時間</i>)
linuxnssScannedFiles	.3.1.202.101	スキャン済みファイル数(カウンター、整数)
linuxnssScannedBytes	.3.1.202.102	スキャン済みバイト数(カウンター、整数)
linuxnssScanErrors	.3.1.202.103	スキャンエラーの発生回数(カウンター、整数)
<i>linuxfirewall</i>	.3.1.203	drweb-firewall(GNU/Linux用)コンポーネントデータ
linuxfirewallState	.3.1.203.1	コンポーネントの現在の状態(整数****)
linuxfirewallExitCode	.3.1.203.2	前回の終了コード(エラーカタログのコードに対応する整数)
linuxfirewallExitTime	.3.1.203.3	前回の終了時刻(<i>UNIX時間</i>)
<i>ctl</i>	.3.1.300	drweb-ctlコンポーネントデータ
ctlState	.3.1.300.1	コンポーネントの現在の状態(整数****)
ctlExitCode	.3.1.300.2	前回の終了コード(エラーカタログのコードに対応する整数)
ctlExitTime	.3.1.300.3	前回の終了時刻(<i>UNIX時間</i>)
license	.3.2	ライセンスのステータス
<i>licenseEsMode</i>	.3.2.1	ライセンスが集中管理サーバーによって付与された(整数:0-いいえ、1-はい)
<i>licenseNumber</i>	.3.2.2	ライセンス番号(整数)
<i>licenseOwner</i>	.3.2.3	ライセンスの所有者(文字列)
<i>licenseActivated</i>	.3.2.4	ライセンスを有効化した日(<i>UNIX時間</i>)
<i>licenseExpires</i>	.3.2.5	ライセンス有効期限(<i>UNIX時間</i>)

*) 脅威のタイプ:



コード	脅威の種類
1	既知のウイルス (<i>known virus</i>)
2	疑わしいオブジェクト (<i>suspicious</i>)
3	アドウェア (<i>adware</i>)
4	ダイヤラー (<i>dialer</i>)
5	ジョークプログラム (<i>joke program</i>)
6	リスクウェア (<i>riskware</i>)
7	ハッキングツール (<i>hacktool</i>)

**) URLのカテゴリー:

コード	脅威の種類
1	感染源 (<i>infectionSource</i>)
2	非推奨 (<i>notRecommended</i>)
3	アダルトコンテンツ (<i>adultContent</i>)
4	暴力 (<i>violence</i>)
5	武器 (<i>weapons</i>)
6	ギャンブル (<i>gambling</i>)
7	麻薬 (<i>drugs</i>)
8	卑猥な表現など (<i>obsceneLanguage</i>)
9	チャット (<i>chats</i>)
10	テロリズム (<i>terrorism</i>)
11	無料メール (<i>freeEmail</i>)
12	ソーシャルネットワーク (<i>socialNetworks</i>)
13	著作権者からの申し立てによって登録されたURL (<i>ownerNotice</i>)
14	オンラインゲーム (<i>onlineGames</i>)
15	アノマイザー (<i>anonymizers</i>)
16	仮想通貨マイニングプール (<i>cryptocurrencyMiningPools</i>)



コード	脅威の種類
17	求人情報サイト (<i>Jobs</i>)
20	ブラックリストに追加済み (<i>blackList</i>)

***) Dr.Webコンポーネントのコード:

コード	コンポーネント
1	Dr.Web ConfigD (<i>drweb-configd</i>)
2	Dr.Web Scanning Engine (<i>drweb-se</i>)
3	Dr.Web File Checker (<i>drweb-filecheck</i>)
4	Dr.Web Updater (<i>drweb-update</i>)
5	Dr.Web ES Agent (<i>drweb-esagent</i>)
6	Dr.Web Network Checker (<i>drweb-netcheck</i>)
7	Dr.Web HTTPD (<i>drweb-httpd</i>)
8	Dr.Web SNMPD (<i>drweb-snmpd</i>)
20	Dr.Web ClamD (<i>drweb-clamd</i>)
21	Dr.Web ICAPD (<i>drweb-icapd</i>)
40	SpIDer Guard for SMB (<i>drweb-smbspider-daemon</i>)
41	SpIDer Gate (<i>drweb-gated</i>)
42	Dr.Web MailD (<i>drweb-maild</i>)
43	Dr.Web LookupD (<i>drweb-lookupd</i>)
50	Dr.Web CloudD (<i>drweb-cloudd</i>)
52	Dr.Web MeshD (<i>drweb-meshd</i>)
60	Dr.Web for Lotus
100	<i>drweb-gui</i> for macOS
102	SpIDer Guard for macOS
103	Dr.Web Firewall for macOS
200	<i>drweb-gui</i> for GNU/Linux



コード	コンポーネント
201	SpIDer Guard(drweb-spider)
202	SpIDer Guard for NSS(drweb-nss)
203	Dr.Web Firewall for Linux(drweb-firewall) for GNU/Linux
300	Dr.Web Ctl(drweb-ctl)
400	Enterprise scanner(Dr.Web for UNIX Internet Gatewaysのコンポーネントではありません)

****)コンポーネントの状態:

コード	ステータス
0	インストールされていません
1	インストールされているが開始されていない
2	起動中
3	実行中
4	終了中

変数の値を直接取得するには、snmpwalkユーティリティを使用します。

```
$ snmpwalk -Os -c <community> -v <SNMP version> <host address> <OID>
```

たとえば、ローカルホストで検出された脅威に関する統計を取得するには、次のコマンドを使用します(Dr.Web SNMPDの設定がデフォルト値に設定されている場合)。

```
$ snmpwalk -Os -c public -v 2c 127.0.0.1 .1.3.6.1.4.1.29690.2.2.1
```



Dr.Web MeshD

Dr.Web MeshDは、「ローカルクラウド」にインストールされたDr.Web for UNIX Internet Gatewaysを持つホストを含むエージェントです。この製品は、インストール済みのDr.Web for UNIX製品にホストを接続します。このクラウドを利用すると、次のタスクを解決できます。

- 複数のクラウドホストによる他のファイルスキャンサービスの提供(スキャンコアサービス)。
- ウイルスデータベースの更新をクラウドホスト間で配布する。

インストール済みのDr.Web for UNIX製品にホストを接続するには、Dr.Web MeshDコンポーネントをすべてのホストにインストールする必要があります。このコンポーネントによってクラウドにホストが組み込まれます。クラウド内のホストの権限と、ホストが使用するクラウド機能は、Dr.Web MeshD設定で簡単に設定できます。

データは、保護されたSSHチャンネルを介して他のクラウドホストと共有されます。

動作原理

このセクションの内容

- [接続タイプ](#)
- [動作モード](#)
- [サービス](#)

Dr.Web MeshDは、Dr.Web for UNIX Internet Gatewaysがインストールされているホストと他のクラウドホスト間のインタラクションを調整します。

接続タイプ

Dr.Web MeshDでは次の接続タイプを使用します。

- **クライアント(サービス)** - Dr.Web MeshDが他のクラウドホストに接続するために使用されます。これらのホストは、指定したホストによって提供されるサービスのクライアントです。



ホスト上で動作し、同じホスト上で動作するDr.Web MeshDを介してクラウド提供のサービスにアクセスするDr.Web for UNIX Internet Gatewaysのコンポーネントは、ローカルのUNIXソケットを介してクライアントに接続します。その場合、クライアント接続は使用されません。

- **パートナー(ピアツーピア)** - ピア(サービス内)パートナークラウドホストとのインタラクションのためにDr.Web MeshDによって使用されます。通常、このような横方向の接続は、クラウドでやり取りする際の負荷の軽減や分散の他、クラウドホストの同期に使用されます。
- **アップリンク** - このホスト(クライアント)をクラウドホスト(サービスプロバイダー)に接続する際に、Dr.Web MeshDによって使用されます(ウイルスデータベースの更新の配布、スキャンのためのファイル転送など)。

使用する3つの種類の接続はすべて、それぞれのクラウドサービスに対して個別に設定されます。さらに同じホストを、サービス内でクライアントの要求(最新の更新を提供するなど)を処理するサーバーとして、および別のサービス内(リモートファイルスキャンなど)のクライアントとして設定できます。



クラウド内では、ホストは安全なSSHプロトコルを介して承認済みのインタラクションを実行します。つまり、ホスト間通信のすべての側面が常に相互認証されます。認証には、[RFC 4251](#)に従ってホストキーが使用されます。ローカルコンポーネントからのクライアント接続は常に信頼済みと見なされます。

動作モード

Dr.Web MeshDはデーモンモードで動作させることも、ローカルホストにある他のDr.Web for UNIX Internet Gatewaysコンポーネントからの要求で実行することもできます。Dr.Web MeshDがクライアント接続を提供するように設定されており(つまり、ListenAddressパラメータが空でなく)、少なくとも1つのサービスがアクティブ化されている場合、Dr.Web MeshDはデーモンとして起動し、クライアントからの接続を待機します。またDr.Web MeshDは、リクエストに応じて、たとえば次のコマンドを実行するときに、ローカルホストで有効化できます。

```
$ drweb-ctl update --local-cloud
```

Dr.Web MeshDがクライアント接続を処理するように設定されておらず(ListenAddressパラメータが空で)、IdleTimeLimitパラメータで指定された期間中にDr.Web MeshDへのリクエストがない場合、コンポーネントは自動的に終了します。

サービス

更新を交換する(更新)

このサービスを使用すると、ホストはウイルスやその他のデータベースの更新をサブスクライブし、更新に関する通知を送信し、クラウドホスト間で更新ファイルをアップロードして共有できます。サービス設定は、Update*パラメータを使用して設定できます。

標準のサービス使用法では、Dr.Web MeshDがインストールされており、会社のローカルネットワーク内の複数のマシン(サービスのクライアント)で更新を取得する機能が有効になっていると想定しています。一般的なクライアント設定は次のとおりです。

```
...
[MeshD]
UpdateChannel = On
UpdateUplink = <server address>
ListenAddress =
...
[Update]
UseLocalCloud = Yes
...
```

更新を配布するローカルサーバーでは、次の設定が指定されています。

```
UpdateChannel = On
UpdateUplink =
ListenAddress = <address>: <port>
```

ここで、クライアントのアップリンク接続の<server address>は、サーバーホストがクライアント接続を管理するために使用する<address>および<port>を参照する必要があります。



ホストの1つが更新サーバー（ローカルクラウドの外部：Dr.Web GUS更新サーバーまたは集中管理サーバー）から更新されている場合、ホストは必要なすべてのクライアントに通知を送信し（ホストが更新交換サーバーとして設定されている場合）、サーバーホストに、ホストから配布可能なファイルの新しいリストを送信します。通知を受信すると、クライアントホストはサーバーからの更新のダウンロードをリクエストできます。次に、クライアントからファイルをリクエストしてローカルに保存するか、サーバーからファイルをリクエストした他のクライアントに送信できません。

このシナリオでは、クライアントが異なるタイミングでDr.Web GUSにリクエストを送信するため、更新の遅延が短縮します。そのため、最初に更新されたクライアントは、必要なすべてのクラウドホストに最新の更新ファイルをすばやく配信します。また、トラフィック量とDr.Web GUSの負荷も軽減されます。



ローカルクラウドを更新の配布に使用する場合、Dr.Web MeshDに加えて、ホストにはDr.Web Updaterコンポーネントが含まれている必要があることに注意してください。

リモートファイルスキャン（エンジン）

このサービスでは、Dr.Web Scanning Engineを使用してリモートファイルをスキャンできます。クライアントホストはスキャン用のファイルをサーバーホストに送信し、サーバーホストはファイルスキャン用のサービスを提供します。一般的なクライアント**設定**は次のとおりです。

```
...
[MeshD]
EngineChannel = On
EngineUplink = <server address>
ListenAddress =
...
```

ローカルスキャンサーバーでは、次の設定が指定されています。

```
EngineChannel = On
EngineUplink =
ListenAddress = <address>: <port>
```

ここで、クライアントのアップリンク接続の<server address>は、サーバーホストがクライアント接続を管理するために使用する<address>および<port>を参照する必要があります。

スキャンするファイルを送信する（ファイル）

この機能は使用されません（リモートスキャンはEngineサービス内で提供されます）。

URLチェック

このサービスでは、サーバーホストを使用して、潜在的に危険で推奨されないカテゴリーに属するURLをチェックできます。クライアントホストは、チェックするURLをサーバーホストに送信します。一般的なクライアント**設定**は次のとおりです。



```
...  
[MeshD]  
UrlChannel = On  
UrlUplink = <server address>  
ListenAddress =  
...
```

URLチェックに使用されるローカルサーバーでは、次の設定が指定されています。

```
UrlChannel = On  
UrlUplink =  
ListenAddress = <address>: <port>
```

ここで、クライアントのアップリンク接続の<server address>は、サーバーホストがクライアント接続を管理するために使用する<address>および<port>を参照する必要があります。

コマンドライン引数

Dr.Web MeshDを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-meshd [<parameters>]
```

Dr.Web MeshDは次のオプションを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了します。 短縮形：-h 引数：なし
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了するように指示します。 短縮形：-v 引数：なし

例：

```
$ /opt/drweb.com/bin/drweb-meshd --help
```

このコマンドは、Dr.Web MeshDに関する簡単なヘルプ情報を出力します。

スタートアップノート

このコンポーネントは、自律モードで(他のコンポーネントから自律的に)OSのコマンドラインから直接起動することはできません。必要に応じて[Dr.Web ConfigD](#)設定デーモンによって自動的に起動されます。コンポーネントの動作を管理するには、Dr.Web for UNIX Internet Gateways用のコマンドラインベース管理ツール[Dr.Web Ctl](#)を使用できます(これはdrweb-ctl1[コマンド](#)を使用して呼び出されます)。



コマンドラインから製品のこのコンポーネントに関するドキュメントを要求するには、`man 1 drweb-meshd`コマンドを使用します。

設定パラメータ

このコンポーネントは、Dr.Web for UNIX Internet Gatewaysの統合された設定ファイルの [MeshD] セクションで指定されている設定パラメータを使用します。

セクションには以下のパラメータが含まれています。

パラメータ	説明
LogLevel <i>{logging level}</i>	コンポーネントのロギングレベル。 パラメータの値が指定されていない場合は、[Root] セクションの DefaultLogLevel パラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントのロギング方式。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行パス。 デフォルト値: <opt_dir>/bin/drweb-meshd <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-meshd• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-meshd
DebugSsh <i>{Boolean}</i>	ロギングレベルが LogLevel = Debug の場合、ホスト上で動作している Dr.Web MeshD が送受信した SSH プロトコルメッセージ (メッセージとデータの転送に使用) のロギングを実行します。 デフォルト値: No
IdleTimeLimit <i>{time interval}</i>	コンポーネントの最大アイドル時間。指定された時間が経過すると、コンポーネントはシャットダウンします。 指定可能な値: 10秒 (10s) から 30日 (30d) まで。 None 値が設定されている場合、コンポーネントは永続的に機能します。コンポーネントがアイドル状態になると、SIGTERM シグナルは送信されません。 デフォルト値: 30s
DnsResolverConfPath <i>{path to file}</i>	ドメイン名パーミッション (DNSリゾルバ) のサブシステム設定ファイルへのパス。 デフォルト値: /etc/resolv.conf
ListenAddress <i><IP address>:<port></i>	コンポーネントがクラウドホストからの接続の受信を待機しているクライアント接続のネットワークソケット (アドレスとポート)。これらのホストは、このクラウドホストによって提供されるサービスのクライアントです。



パラメータ	説明
	<p>コンポーネントがIPv6インターフェースをリッスンし、IPv6経由でクラウドクライアントホストを検出するためには、このパラメータを設定する必要があります。 値が指定されていない場合、コンポーネントはクライアントからの要求を受け取りません。</p> <p>デフォルト値：(未設定)</p>
UpdateChannel {On / Off}	<p>このホスト上で動作するDr.Web MeshDコンポーネントを有効または無効にし、クラウドのホスト間でウイルスデータベースの更新を交換します(たとえば、他のクラウドホストからウイルスデータベースの更新を取得し、新しい更新をクラウドに送信します)。</p> <p>このパラメータがOnに設定されている場合、コンポーネントDr.Web MeshDはDr.Web ConfigD設定デーモンによって自動的に起動されます。</p> <p>デフォルト値：On</p>
UpdateUplink {address}	<p>このホストにURLチェックサービスを提供するサーバーとして機能するDr.Web MeshDの上位ホストのアドレス。</p> <p>使用可能な値：</p> <ul style="list-style-type: none">• 指定なし - サーバーがサービスに設定されておらず、Dr.Web MeshDはどこにも接続されません。• <IP address>:<port> - Dr.Web MeshDは指定されたアドレスとポートでサーバーに接続します。• dns:<service name>[:<domain>] - サーバーのアドレスとポートは、<domain>DNSドメインのSRVレコードを検索することで指定されます。<domain>が指定されていない場合、DNSリゾルバ設定ファイルのドメインが使用されます(パスはResolverConfPathで指定されます)。このドメインは、最後に検出されたドメインに応じて、searchまたはdomainフィールドから取得されます。• discover - 検出メカニズムによって上位ホストを検索します。 <p>デフォルト値：(指定なし)</p>
UpdateDebugIpc {Boolean}	<p>ロギングレベルがLogLevel = Debugの場合は、更新の交換サービスのログにデバッグ情報を出力します。</p> <p>デフォルト値：No</p>
UpdateTraceContent {Boolean}	<p>ロギングレベルがLogLevel = Debugの場合は、更新の交換サービスのログに送信済みデータを出力します。</p> <p>デフォルト値：No</p>
FileChannel {On / Off}	<p>このホストで動作するDr.Web MeshDコンポーネントがファイル交換に参加できるようにするオプションを有効または無効にします。</p> <p>このパラメータがOnに設定されている場合、コンポーネントDr.Web MeshDはDr.Web ConfigD設定デーモンによって自動的に起動されます。</p> <p>デフォルト値：On</p>
FileUplink {address}	<p>このホストのファイルをスキャンするサーバーとして機能するDr.Web MeshDの上位ホストのアドレス。</p>



パラメータ	説明
	<p>使用可能な値：</p> <ul style="list-style-type: none">• <i>指定なし</i> - サーバーがサービスに設定されておらず、Dr.Web MeshDはどこにも接続されません。• <i><IP address>:<port></i> - Dr.Web MeshDは指定されたアドレスとポートでサーバーに接続します。• <i>dns:<service name>[:<domain>]</i> - サーバーのアドレスとポートは、<domain>DNSドメインのSRVレコードを検索することで指定されます。<domain>が指定されていない場合、DNSリゾルバ設定ファイルのドメインが使用されます（パスはResolverConfPathで指定されます）。このドメインは、最後に検出されたドメインに応じて、searchまたはdomainフィールドから取得されます。• <i>discover</i> - 検出メカニズムによって上位ホストを検索します。 <p>デフォルト値：(<i>指定なし</i>)</p>
FileDebugIpc {Boolean}	<p>ロギングレベルがLogLevel = Debugの場合は、ファイル交換サービスのログにデバッグ情報を出力します。</p> <p>デフォルト値：No</p>
EngineChannel {On / Off}	<p>このホストで動作するDr.Web MeshDコンポーネントがスキャンエンジンサービスの提供に参加できるようにするオプションを有効または無効にします。</p> <p>このパラメータがOnに設定されている場合、コンポーネントDr.Web MeshDはDr.Web ConfigD設定デーモンによって自動的に起動されます。</p> <p>デフォルト値：On</p>
EngineUplink {address}	<p>このホストにスキャンエンジンサービスを提供するスキャンサーバーとして機能するDr.Web MeshDの上位ホストのアドレス。</p> <p>使用可能な値：</p> <ul style="list-style-type: none">• <i>指定なし</i> - サーバーがサービスに設定されておらず、Dr.Web MeshDはどこにも接続されません。• <i><IP address>:<port></i> - Dr.Web MeshDは指定されたアドレスとポートでサーバーに接続します。• <i>dns:<service name>[:<domain>]</i> - サーバーのアドレスとポートは、<domain>DNSドメインのSRVレコードを検索することで指定されます。<domain>が指定されていない場合、DNSリゾルバ設定ファイルのドメインが使用されます（パスはResolverConfPathで指定されます）。このドメインは、最後に検出されたドメインに応じて、searchまたはdomainフィールドから取得されます。• <i>discover</i> - 検出メカニズムによって上位ホストを検索します。 <p>デフォルト値：(<i>指定なし</i>)</p>
EngineDebugIpc {Boolean}	<p>ロギングレベルがLogLevel = Debugの場合は、スキャンサービスのログにデバッグ情報を出力します。</p> <p>デフォルト値：No</p>
UrlChannel {On / Off}	<p>このホストで動作するDr.Web MeshDコンポーネントがURLチェックサービスの提供に参加できるようにするオプションを有効または無効にします。</p>



パラメータ	説明
	デフォルト値 : On
UrlUplink {address}	<p>このホストにURLチェックサービスを提供するサーバーとして機能するDr.Web MeshDの上位ホストのアドレス。</p> <p>使用可能な値 :</p> <ul style="list-style-type: none">• 指定なし - サーバーがサービスに設定されておらず、Dr.Web MeshDはどこにも接続されません。• <IP address>:<port> - Dr.Web MeshDは指定されたアドレスとポートでサーバーに接続します。• dns:<service name>[:<domain>] - サーバーのアドレスとポートは、<domain>DNSドメインのSRVレコードを検索することで指定されます。<domain>が指定されていない場合、DNSリゾルバ設定ファイルのドメインが使用されます (パスはResolverConfPathで指定されます)。このドメインは、最後に検出されたドメインに応じて、searchまたはdomainフィールドから取得されます。• discover - 検出メカニズムによって上位ホストを検索します。 <p>デフォルト値 : (指定なし)</p>
DiscoveryResponderPort {port number}	<p>上位ホストがUDPプロトコルを介して設定されたクライアントの要求に応答するポート。</p> <p>検出メカニズムは、ListenAddress値が設定されている場合にのみ有効になります。</p> <p>デフォルト値 : 18008</p>
UrlDebugIpc {Boolean}	<p>ロギングレベルがLogLevel = Debugの場合、デバッグ情報をURLチェックサービスのログに出力します。</p> <p>デフォルト値 : No</p>



Dr.Web for UNIX Internet Gatewaysの現在のバージョンでは、ファイル送信サービスは使用されません。代わりに、Engineスキャンエンジンサービスを使用します。

Dr.Web URL Checker

Dr.Web URL Checkerは、URLが望ましくないカテゴリーや悪意のあるカテゴリーに属していないかどうかをチェックするために、他のコンポーネントが使用する補助コンポーネントです。

Dr.Web URL Checkerは次のコンポーネントによって使用されます。

- [Dr.Web HTTPD](#)
- [Dr.Web MeshD](#)
- [SpIDer Gate](#)
- [Dr.Web ICAPD](#)



動作原理

Dr.Web URL Checkerコンポーネントは、URLが望ましくないカテゴリーや潜在的に危険なカテゴリーに属していないかチェックするために、他のコンポーネントが使用します。

このチェックは、専用のリンクベースを使用するか、Dr.Web CloudDサービスを使用して実行できます。Dr.Web CloudDサービスを使用するには、次のコマンドを実行します。

```
$ drweb-ctl cfset Root.UseCloud Yes
```

ユーザーがDr.Web URL Checkerを起動することはできません。他のコンポーネントのリクエストに応じて、Dr.Web ConfigD構成管理デーモンによって起動されます。

コマンドライン引数

Dr.Web URL Checkerを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-urlcheck [<parameters>]
```

Dr.Web URL Checkerは次のオプションを処理できます。

パラメータ	説明
--help	機能: コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了します。 短縮形: -h 引数: なし
--version	機能: このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了します。 短縮形: -v 引数: なし

例:

```
$ /opt/drweb.com/bin/drweb-urlcheck --help
```

このコマンドは、URL Checkerに関する簡単なヘルプ情報を出力します。

スタートアップノート

このコンポーネントは、自律モードで(他のコンポーネントから自律的に)OSのコマンドラインから直接起動することはできません。必要に応じてDr.Web ConfigD設定デーモンによって自動的に起動されます。コンポーネントの動作を管理するには、Dr.Web for UNIX Internet Gateways用のコマンドラインベース管理ツールDr.Web Ctlを使用できます(これはdrweb-ctlコマンドを使用して呼び出されます)。



コマンドラインから製品のこのコンポーネントに関するドキュメントを要求するには、`man 1 drweb-urlcheck`コマンドを使用します。

設定パラメータ

このコンポーネントは、Dr.Web for UNIX Internet Gatewaysの統合された設定ファイルの[Urlcheck]セクションで指定されている設定パラメータを使用します。

セクションには以下のパラメータが含まれています。

パラメータ	説明
LogLevel <i>{logging level}</i>	コンポーネントのロギングレベル。 パラメータの値が指定されていない場合は、[Root]セクションのDefaultLogLevelパラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントのロギング方式。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行パス。 デフォルト値: <opt_dir>/bin/drweb-urlcheck • GNU/Linuxの場合: /opt/drweb.com/bin/drweb-urlcheck • FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-urlcheck
RunAsUser <i>{UID user name}</i>	その権限によりコンポーネントを実行するユーザーの名前。このユーザー名は、ユーザーのUIDまたはユーザーのログインとして指定できます。ユーザー名が数字で構成されている場合(つまりUIDに似ている場合)は、「name:」というプレフィックスを付けて指定します。たとえば、RunAsUser = name:123456です。 ユーザー名が指定されていない場合、コンポーネント操作は開始後にエラーが発生して終了します。 デフォルト値: drweb
IdleTimeLimit <i>{time interval}</i>	コンポーネントの最大アイドル時間。指定された時間が経過すると、コンポーネントはシャットダウンします。 指定可能な値: 10秒(10s)から30日(30d)まで。 None値が設定されている場合、コンポーネントは永続的に機能します。コンポーネントがアイドル状態になると、SIGTERMシグナルは送信されません。 デフォルト値: 30s



Dr.Web CloudD

Dr.Web CloudDコンポーネントはDr.Web Cloud (Doctor Webのクラウドサービス)を参照します。Dr.Web Cloudサービスは、検出された脅威に関する最新情報をすべてのDr.Webアンチウイルスソリューションから収集し、ユーザーが望ましくないWebサイトにアクセスするのを防ぎ、Dr.Webウイルスデータベースに記述のない新しい脅威を含んだ感染ファイルからOSを保護します。さらに、Dr.Web Cloudサービスを使用すると、[Dr.Web Scanning Engine](#)スキャンエンジンやインターネットへのアクセスを監視するコンポーネントの誤検知の可能性が少なくなります。

動作原理

このコンポーネントは、指定ファイルのコンテンツにローカルの[Dr.Web Scanning Engine](#)が把握していない脅威がないかスキャンし、指定URLがDoctor WebのWebリソースの定義済みカテゴリーに属するかどうかを確認するよう、Doctor Web Dr.Web Cloudサービスに指示します。またこのコンポーネントは、感染ファイルの検出に関する統計情報と、Dr.Web for UNIX Internet Gatewaysを実行しているOSに関する情報を定期的にDr.Web Cloudに送信します。

Dr.Web CloudDは設定デーモンによって自動的に実行されます。このコンポーネントは、ユーザーまたはDr.Web for UNIX Internet Gatewaysコンポーネントの1つからコマンドを受信したときに実行されます。

このコンポーネントは、ネットワークトラフィックとURL [SpIDer Gate](#)および[Dr.Web ICAPD](#)のスキャンコンポーネントによって、ユーザーがリクエストしたURLのスキャンのために、Dr.Web Cloudサービスへのリクエストに使用されません。

さらに、このコンポーネントはコマンドライン[Dr.Web Ctl](#)(`drweb-ctl`コマンドによって起動)からのDr.Web for UNIX Internet Gateways管理ユーティリティのコマンドによるファイルのスキャン中に使用されます。脅威が検出されると、[Dr.Web Scanning Engine](#)スキャンエンジンがファイルに関するレポートをDr.Web Cloudに送信します。



コマンドライン引数

Dr.Web CloudDを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-cloudd [<parameters>]
```

Dr.Web CloudDは次のオプションを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了します。 短縮形：-h 引数：なし
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了します。 短縮形：-v 引数：なし

例：

```
$ /opt/drweb.com/bin/drweb-cloudd --help
```

このコマンドは、Dr.Web CloudDに関する簡単なヘルプ情報を出力します。

スタートアップノート

このコンポーネントは、自律モードで(他のコンポーネントから自律的に)OSのコマンドラインから直接起動することはできません。必要に応じて、[Dr.Web ConfigD](#)設定デーモンによって自動的に起動されます。コンポーネントの動作を管理するには、Dr.Web for UNIX Internet Gateways用のコマンドラインベース管理ツール [Dr.Web Ctl](#)を使用できます(drweb-ctl [コマンド](#)を使用して呼び出されます)。



コマンドラインから製品のこのコンポーネントに関するドキュメントを要求するには、`man 1 drweb-cloudd`コマンドを使用します。

設定パラメータ

このコンポーネントは、Dr.Web for UNIX Internet Gatewaysの統合された[設定ファイル](#)の[CloudD]セクションで指定されている設定パラメータを使用します。

セクションには以下のパラメータが含まれています。

パラメータ	説明
LogLevel	コンポーネントの ロギングレベル 。



パラメータ	説明
<i>{logging level}</i>	パラメータの値が指定されていない場合は、[Root] セクション の DefaultLogLevelパラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行パス。 デフォルト値: <opt_dir>/bin/drweb-cloudd <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-cloudd• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-cloudd
RunAsUser <i>{UID / user name}</i>	その権限によりコンポーネントを実行するユーザーの名前。このユーザー名は、ユーザーのUIDまたはユーザーのログインとして指定できます。ユーザー名が数字で構成されている場合(つまりUIDに似ている場合)は、「name:」というプレフィックスを付けて指定します。たとえば、RunAsUser = name:123456です。 ユーザー名が指定されていない場合、コンポーネント操作は開始後にエラーが発生して終了します。 デフォルト値: drweb
IdleTimeLimit <i>{time interval}</i>	コンポーネントの最大アイドル時間。指定された時間が経過すると、コンポーネントはシャットダウンします。 指定可能な値: 10秒(10s)から30日(30d)まで。 None値が設定されている場合、コンポーネントは永続的に機能します。コンポーネントがアイドル状態になると、SIGTERMシグナルは送信されません。 デフォルト値: 1h
PersistentCache <i>{On / Off}</i>	Dr.Web Cloud応答のキャッシュをディスクへ保存することを有効または無効にします。 デフォルト値: Off
DebugSdk <i>{Boolean}</i>	詳細なDr.Web Cloudメッセージをデバッグレベルでログファイルに含めるかどうかを示します(LogLevel = DEBUG)。 デフォルト値: No



Dr.Web LookupD

Dr.Web LookupDコンポーネントは、LDAPプロトコルを使用してデータを取得するために、外部ソース(LDAPプロトコルのインタラクションをサポートする、テキストファイル、リレーショナルデータベース、ディレクトリサービス)を参照するように設計されています。受信したデータはルールで使用され、それに従ってネットワーク接続がスキャンされます(ユーザーの承認のチェックなど)。このデータは、特定の条件が満たされた場合にURLへのアクセスをブロックするためにも使用されます。

コンポーネントの設定では、いくつかのデータソースに接続するためのパラメータを指定できます。Dr.Web LookupDは、Dr.Web for UNIX Internet Gatewaysのいずれかのコンポーネントからデータリクエストを受信した場合にのみ、必要なデータソースに接続します。

Dr.Web LookupDでは次のデータソースへの参照がサポートされます。

- テキストファイル(*AllMatch*、*Mask*、*Regex*、*Cidr*モード)。
- リレーショナルデータベース(MySQL、PostgreSQL、SQLite)。
- Redisデータストレージ。
- ディレクトリサービス(Active Directoryや、LDAP経由のアクセスを提供するその他のサービス、たとえばOpenLDAPなど)。

LDAPプロトコルによるデータの共有は、オープンチャネルまたは保護されたチャネル経由でSSL/TLSを適用することで実行できます。安全な接続を使用するには、Dr.Web LookupDに適切なSSL証明書とキーを提供する必要があります。SSLキーと証明書を生成する必要がある場合は、`openssl`ユーティリティを使用できます。

`openssl`ユーティリティを使用して証明書とプライベートキーを生成する方法の例については、[付録E. SSL証明書](#)を生成するのセクションを参照してください。

動作原理

このコンポーネントは、テキストファイル、リレーショナルデータベース、ネットワークストレージ、LDAPプロトコルをサポートするディレクトリサービス(Active Directoryなど)にデータをリクエストするように設計されています。受信したデータ(ユーザーのIDや権限など)は、Dr.Web for UNIX Internet Gatewaysのコンポーネントに転送され、さまざまなルールでスキャンに使用されます(ユーザーがリクエストしたURLなどにアクセスを許可するなど)。



このマニュアルではリレーショナルデータベース、Redisストレージ、ディレクトリサービス、LDAPプロトコルの動作原理については説明しません。必要に応じて、対応する参考資料を参照してください。

Dr.Web LookupDコンポーネントは、必要に応じて(データのリクエストを受信するときに)[Dr.Web ConfigD](#)設定デーモンによって自動的に起動されます。

特定のコンポーネントからのデータ受信に関するリクエストが到着すると、[Dr.Web ConfigD](#)設定デーモンがDr.Web LookupDを起動します(起動されていない場合)。次に、コンポーネントはリクエストされたデータソースからリクエストを実行し、レスポンスを返します。リクエストに応じて応答は異なり、所定の検索条件に従ってデータソースから取得された、特定の検索条件を満たす文字列のリスト、または所定の条件に一致する文字列が検索結果に含まれているかどうかを示す論理値(trueまたはfalse)で構成されます。

Dr.Web LookupDの設定で指定できるデータソースの数に制限はありません。クライアントコンポーネントは、データ取得リクエストを作成するときに、データソースを指定する必要があります。Dr.Web LookupDは起動後し



ばらくの間、新しいリクエストを待機します。それ以上リクエストがない場合は、待機期間が経過した後、Dr.Web LookupDは自動的にシャットダウンします。

Dr.Web for UNIX Internet Gatewaysのその他のコンポーネントは、Dr.Web LookupDを使用するための基本の動作として、それらのコンポーネントの動作ルールで指定されている条件の妥当性を確認するために必要なデータを取得します。ルールの適用可能性と条件の妥当性をチェックするときに、Dr.Web LookupDに対するデータリクエストが自動的に実行されます。

テキストファイル処理の特性

1. テキストファイルを処理するとき、文字列の先頭と末尾のスペースは破棄されます。空白行と最初の文字が「#」で始まる行は無視されます。
2. テキストファイルは不変のデータソースと見なされ、その内容はメモリ内に完全にキャッシュされます。さらに、検証のためのこれらのファイルに対するリクエストの結果もキャッシュされます。そのため、ソースファイルが変更されている場合は、`drweb-ctl`の`reload`コマンドなどを使用してDr.Web ConfigDコンポーネントにHUPシグナルを送信することで、Dr.Web LookupDに設定を再読み込みさせる必要があります。

MySQL接続の状況

MySQL接続の前に、MySQLファイル設定の`[client]`セクションのパラメータがデフォルトで読み取られます（ファイル検索は、`/etc/my.cnf`、`/etc/mysql/my.cnf`、`/etc/alternatives/my.cnf`のパスで行われます）。

コマンドライン引数

Dr.Web LookupDを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-lookupd [<parameters>]
```

Dr.Web LookupDは次のパラメータを処理できます。

パラメータ	説明
<code>--help</code>	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了するように指示します。 短縮形： <code>-h</code> 引数：なし
<code>--version</code>	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了するように指示します。 短縮形： <code>-v</code> 引数：なし

例：

```
$ /opt/drweb.com/bin/drweb-lookupd --help
```

このコマンドは、Dr.Web LookupDに関する簡単なヘルプ情報を出力します。



スタートアップノート

このコンポーネントは、自律モードで(他のコンポーネントから自律的に)OSのコマンドラインから直接起動することはできません。必要に応じて[Dr.Web ConfigD](#)設定デーモンによって自動的に起動されます。コンポーネントの動作を管理するには、Dr.Web for UNIX Internet Gateways用のコマンドラインベース管理ツール[Dr.Web Ct](#)を使用できます(これはdrweb-ctlコマンドを使用して呼び出されます)。



コマンドラインから製品のこのコンポーネントに関するドキュメントを要求するには、`man 1 drweb-lookupd`コマンドを使用します。

設定パラメータ

このセクションの内容

- [コンポーネントパラメータ](#)
- [データソースセクション](#)
- [新しいデータソース用のセクションの追加](#)

このコンポーネントは、Dr.Web for UNIX Internet Gatewaysの統合された[設定ファイル](#)の[LookupD]セクションで指定されている設定パラメータを使用します。

コンポーネントパラメータ

セクションには以下のパラメータが含まれています。

パラメータ	説明
LogLevel <i>{logging level}</i>	コンポーネントの ロギングレベル 。 パラメータの値が指定されていない場合は、[Root] セクション のDefaultLogLevelパラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行パス。 デフォルト値: <opt_dir>/bin/drweb-lookupd <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-lookupd• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-lookupd
RunAsUser <i>{UID user name}</i>	このパラメータは、コンポーネントを実行するユーザー名を決定します。ユーザー名は、ユーザーのUIDまたはユーザーのログインとして指定できます。ユーザー名が数字で構成されている場合(つまりUIDに似ている場合)は、「name:」というプレフィックスを付けて指定します。たとえば、RunAsUser = name:123456です。



パラメータ	説明
	<p>ユーザー名が指定されていない場合、コンポーネント操作は開始後にエラーが発生して終了します。</p> <p>デフォルト値: drweb</p>
IdleTimeLimit {time interval}	<p>コンポーネントの最大アイドル時間。指定された時間が経過すると、コンポーネントはシャットダウンします。</p> <p>指定可能な値: 10秒 (10s) から30日 (30d) まで。 None値が設定されている場合、コンポーネントは永続的に機能します。コンポーネントがアイドル状態になると、SIGTERMシグナルは送信されません。</p> <p>デフォルト値: 30s</p>
DebugLibldap {Boolean}	<p>libldapライブラリのデバッグメッセージもデバッグレベルでログファイルに含めるかどうかを示します (つまり、LogLevel = DEBUGの場合)。</p> <p>デフォルト値: No</p>
LdapCheckCertificate {No / Allow / Try / Yes}	<p>SSL/TLS経由のLDAP接続の証明書検証モード。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• No - サーバーの証明書を要求しない。• Allow - サーバーの証明書を要求する。証明書が提供されない場合、セッションは通常どおりに続行されます。サーバーの証明書が提供されてもスキャンできない (対応するルート証明書が見つからない) 場合、その証明書は無視され、セッションは通常どおりに続行されます。• Try - サーバーの証明書を要求する。証明書が提供されない場合、セッションは通常どおりに続行されます。サーバーの証明書が提供されても確認できない (対応するルート証明書が見つからない) 場合、セッションは終了します。• Yes - サーバーの証明書を要求する。証明書が提供されないか、スキャンできない場合 (対応するルート証明書が見つからない場合)、セッションは終了します。 <p>LDAPデータソースの場合、この証明書検証モードは、ldaps://スキームまたはStartTLS拡張機能が使用されるときにURLの処理方法に影響します。ADデータソースの場合は、対応するセクションでUseSSL=Yesが指定されていると (以下参照)、サーバーへの接続に影響します。</p> <p>デフォルト値: Yes</p>
LdapCertificatePath {path to file}	<p>安全なSSL/TLS接続を介したLDAPサーバーへの接続 (Active Directory) に使用されるSSL証明書へのパス。</p> <p>証明書ファイルとプライベートキーファイル (後述のパラメータで指定されます) は、一致するペアを形成する必要があります。</p> <p>デフォルト値: (未設定)</p>
LdapKeyPath {path to file}	<p>安全なSSL/TLS接続を介したLDAPサーバーへの接続 (Active Directory) に使用されるプライベートキーへのパス。</p> <p>証明書ファイルとプライベートキーファイル (上記のパラメータで指定されます) は、一致するペアを形成する必要があります。</p>



パラメータ	説明
	デフォルト値：(未設定)
LdapCaPath {path}	<p>SSL/TLSを介したLDAPプロトコルによるデータの共有に信頼して使用できる、信頼できるルート証明書のシステムリストを含むディレクトリまたはファイルへのパス。</p> <p>デフォルト値：<path to the list of trusted certificates>。パスは、お使いのGNU/Linuxディストリビューションに依存します。</p> <ul style="list-style-type: none">• Astra Linux、Debian、Linux Mint、SUSE Linux、Ubuntuの場合、通常はパス/etc/ssl/certs/です。• CentOSとFedoraの場合はパス/etc/pki/tls/certs/ca-bundle.crtです。• 他のディストリビューションでは、コマンドopenssl version -dの実行結果によってパスを定義できます。• コマンドが使用できない場合、またはOSディストリビューションを特定できない場合は、値/etc/ssl/certs/が使用されます。
DbIdleTimeout {time interval}	<p>データベース(またはRedisストレージ)への確立された接続がアイドル状態になっている場合に、その接続を切断するまでのタイムアウト期間。</p> <p>デフォルト値：5m</p>
MysqlDefaultConn {URL}	<p>MySQLデータベースに接続するためのパラメータをデフォルトで設定するURI。</p> <p>使用可能な値：</p> <ul style="list-style-type: none">• tcp://[<user>[:<password>]@][<host>][:<port>][/<database name>][?<parameter>=<value>[&...]]• unix://[<user>[:<password>]@]<path to socket>[:<database name>][?<parameter>=<value>[&...]] <p>URI要件に注意してください。</p> <p>デフォルト値：(未設定)</p>
PqDefaultConn {URL}	<p>PostgreSQLデータベースに接続するためのパラメータをデフォルトで設定するURI。</p> <p>使用可能な値：</p> <ul style="list-style-type: none">• tcp://[<user>[:<password>]@][<host>][:<port>][/<database name>][?<parameter>=<value>[&...]]• unix://[<user>[:<password>]@]<path to socket>[:<database name>][?<parameter>=<value>[&...]] <p>URI要件に注意してください。</p> <p>デフォルト値：(未設定)</p>
SqliteDefaultConn {path to file}	<p>デフォルトのSQLiteデータベースファイルへのパス(file://スキームプレフィックスを指定)。</p> <p>デフォルト値：(未設定)</p>
RedisDefaultConn {URL}	<p>Redisデータベースへの接続パラメータをデフォルトで設定するURLです。</p>



パラメータ	説明
	<p>使用可能な値:</p> <ul style="list-style-type: none"> tcp://[<password>@][<host>][:<port>][/<database index>] unix://[<password>@] <socket path>[:<database index>] <p>URI要件に注意してください。</p> <p>デフォルト値:(未設定)</p>

データベース接続のURI要件

1. tcp:およびunix:スキームプレフィックスのみを使用します(ローカルUNIXソケットの場合)。データベース固有のプレフィックス(postgresql:およびmysql:など)はサポートしていません。SQLiteデータベースファイルへのパスは、file://スキームプレフィックスで指定されます。
2. <host>フィールドがURIで指定されていないか、localhostホストが指定されている場合、ホストアドレス127.0.0.1が置き換えられます。この場合、MySQLおよびPostgreSQLデータベースでは、ネットワーク接続が指定されているにもかかわらず、ローカルUNIXソケットを介してデフォルトで接続が確立されます。
3. URIフィールド(<user>、<password>、<database name>など)または接続パラメータ文字列に特殊文字(スペース、列など)が含まれている場合は、次のように16進コーディングを使用します。たとえば、
 - スペース - "%20"
 - ':' - "%3A"
 - '/' - "%2F"
 - '@' - "%40"
 - '%' - "%25"
4. MySQLの場合、接続パラメータ文字列には次のパラメータのみを含めることができます。

パラメータ名	データベースドキュメントの文字・記号	タイプ	説明
init	<i>MYSQL_INIT_COMMAND</i>	文字列	データベースへの接続後に実行するSQLコマンド
compression	<i>MYSQL_OPT_COMPRESS</i>	論理	データ圧縮を使用する
connect-timeout	<i>MYSQL_OPT_CONNECT_TIMEOUT</i>	整数	未使用の接続を切断するためのタイムアウト(秒)
reconnect	<i>MYSQL_OPT_RECONNECT</i>	論理	自動再接続を許可または拒否する
read-timeout	<i>MYSQL_OPT_READ_TIMEOUT</i>	整数	サーバーからのパケット受信のタイムアウト(秒)
write-timeout	<i>MYSQL_OPT_WRITE_TIMEOUT</i>	整数	パケットをサーバーに送信するためのタイムアウト(秒)



パラメータ名	データベースドキュメントの文字・記号	タイプ	説明
charset	<i>MYSQL_SET_CHARSET_NAME</i>	文字列	デフォルトの接続に使用される文字エンコーディングの名前
plugin-dir	<i>MYSQL_PLUGIN_DIR</i>	文字列	プラグインを格納するサーバーのディレクトリへのパス
nonblock	<i>MYSQL_OPT_NONBLOCK</i>	整数	ブロック以外のI/O操作のスタックサイズ
ssl-key	<i>MYSQL_OPT_SSL_KEY</i>	文字列	安全な接続を確立するために使用されるプライベートキー（PEM形式）へのパス
ssl-cert	<i>MYSQL_OPT_SSL_CERT</i>	文字列	安全な接続を確立するために使用されるパブリックキー証明書（PEM形式）へのパス
ssl-ca	<i>MYSQL_OPT_SSL_CA</i>	文字列	信頼できるCA証明書を含むファイル（PEM形式）へのパス
ssl-capath	<i>MYSQL_OPT_SSL_CAPATH</i>	文字列	信頼できるCA証明書を含むディレクトリへのパス（PEM形式）
ssl-cipher	<i>MYSQL_OPT_SSL_CIPHER</i>	文字列	安全な接続でサポートされている暗号化アルゴリズムのリスト
ssl-crl	<i>MYSQL_OPT_SSL_CRL</i>	文字列	失効した証明書を含むファイル（PEM形式）へのパス
ssl-crlpath	<i>MYSQL_OPT_SSL_CRLPATH</i>	文字列	失効した証明書を含むディレクトリへのパス（PEM形式）
ssl-fp	<i>MARIADB_OPT_SSL_FP</i>	文字列	有効なサーバー証明書のSHA1ハッシュ
ssl-fp-list	<i>MARIADB_OPT_SSL_FP_LIST</i>	文字列	有効なサーバー証明書のSHA1ハッシュを含むファイルへのパス
tls-passphrase	<i>MARIADB_OPT_TLS_PASSPHRASE</i>	文字列	パスワードで保護されたクライアントプライベートキーのパスワード



パラメータ名	データベースドキュメントの文字・記号	タイプ	説明
tls-version	<i>MARIADB_OPT_TLS_VERSION</i>	文字列	サポートされるTLSバージョンのリスト
server-verify-cert	<i>MYSQL_OPT_SSL_VERIFY_SERVER_CERT</i>	論理	サーバー証明書の検証を許可または禁止する
server-public-key-path	<i>MYSQL_SERVER_PUBLIC_KEY</i>	文字列	RSAサーバーパブリックキーを含むファイル (PEM形式) へのパス

データベースのドキュメントでのパラメータの詳細については、https://mariadb.com/kb/en/mysql_options/を参照してください。

5. PostgreSQLデータベースについては、<https://www.postgresql.org/docs/current/libpq-connect.html#LIBPQ-PARAMKEYWORDS>も参照してください。

データソースセクション

設定ファイルには、一般的なセクションである [LookupD] の他、データソースへの接続を記述するセクション (各接続につき1つのセクション) もあります。これらのセクションには、[LookupD. <type>. <name>] というスキームを使用して名前が付けられます。ここで、

- <type> - 接続の種類:
 - LDAP - LDAPを使用するディレクトリサービス用。
 - AD - Active Directoryサービス。
 - AllMatch - *AllMatch*モードのテキストファイル用 (フル認証)。
 - Mask - *Mask*モードのテキストファイル用 (マスク認証)。
 - Regex - *Regex*モードのテキストファイル用 (PCRE標準の正規表現に対する認証)。
 - Cidr - *Cidr*モードのテキストファイル用 (IPアドレスまたはIPアドレス範囲認証)。
 - Pq - PostgreSQLデータベース用。
 - Mysql - Mysqlデータベース用。
 - Sqlite - Sqliteデータベース用。
 - Redis - Redisデータベース用。
- <name> - 接続の一意のID (タグ)。これを使用してルールから接続を参照できます。

たとえば、[LookupD.LDAP.auth1]とします。データソースのセクション内に含まれるパラメータのセットは、接続のタイプによって異なります。データソースセクションの数に制限はありません。

1. LDAPタイプのセクションで使用されるパラメータ

パラメータ	説明
Url <i>{string}</i>	使用されるLDAPサーバーと抽出されるデータを定義するURL。URLは、 RFC 4516 に従って次のスキームに基づいて構築されます。



```
<scheme>: // <host>[: <port>] / <dn>[? <attrs>[? <scope>[? <filter>[? <extensions>]]]]
```

各パラメータは次のとおりです。

<scheme> - サーバーへの接続方法 (許可されるスキーム: ldap、ldaps、ldapi)。

<host>[: <port>] - リクエストを受信するLDAPサーバーアドレス。

<dn> - オブジェクトの識別名。このオブジェクトに関する情報が送信されました。

<attrs> - レコード属性の名前。この値はリクエスト内で受信する必要があります。

<scope> - 検索範囲 (base、one、sub)。

<filter> - 抽出された属性の値に対するフィルター条件。

<extensions> - リクエストで使用されるLDAP拡張子のリスト。

機能

- 属性のリスト <attrs>では、「*」、「+」、「1.1」の任意の特殊文字を使用できます。
- 以下の自動的に解決されるプレースホルダーは、URLの <dn>および <filter>部分で使用できます。
 - \$uは、クライアントコンポーネントによって送信されたユーザー名 (user) に自動的に置き換えられます。
 - \$dは、クライアントコンポーネントによって送信されたドメイン (domain) に自動的に置き換えられます。
 - \$D - dc= <subdomain>, dc= <domain>に変更される <subdomain>, <domain>チェーン。
 - \$\$ - 「\$」文字。
- <filter>条件で特殊文字 (「*」、「(」、「)」、「\」、コードが0の文字など) を通常の文字として使用する必要がある場合、それらの文字は \XX と記述する必要があります。さらに、URL LDAPの特殊文字は、シーケンス %XX を使用してエンコードされます。たとえば、「/」文字の ldapiスキームに従ってURLをローカルLDAPサーバーソケットへのパスの一部として使用する場合、この文字は %2f としてエンコードされます。
- <extensions>で許可される拡張機能として、StartTLSと 1.3.6.1.4.1.1466.20037のみがサポートされます。これらの拡張機能では、保護されたスキームである ldaps を使用することが明示されていない場合でも、TLSメカニズム (つまり、LDAPサーバーとの保護された接続の確立) が使用されます。使用される拡張機能の名前の前に「!」文字がある場合は、TLSを使用する **必要があります**。つまり、安全な接続を確立できない場合には、リクエストは **処理されません**。それ以外の場合には、安全な接続が確立されていなくてもリクエストは処理されます。



指定された拡張機能は、保護された ldaps スキームでは使用できません。詳細については、[RFC 4516](#) または `man ldap_search_ext_s` を参照してください。



	<p>例 :</p> <pre>"ldaps://ds.example.com:990/\$D?givenName,sn,cn?sub?(uid=\$u)" "ldap://ldap.local/o=org,dc=nodomain? ipNetworkNumber?sub?(objectClass=ipNetwork)? !StartTLS"</pre> <p>デフォルト値 : (未設定)</p>
BindDn <i>{string}</i>	<p>ユーザーが認証を受けなければならないLDAPディレクトリ内のオブジェクト。</p> <p>例 : "cn=admin,dc=nodomain"</p> <p>デフォルト値 : (未設定)</p>
BindPassword <i>{string}</i>	<p>LDAPサーバー上での認証に使用するユーザーのパスワード。</p> <p>デフォルト値 : (未設定)</p>
ChaseReferrals <i>{Boolean}</i>	<p>現在のLDAPサーバーがリクエストへの応答として他のLDAPサーバーへの参照を返す場合、その参照に従うようコンポーネントに指示します。</p> <p>デフォルト値 : No</p>

2. ADタイプのセクションで使用されるパラメータ

パラメータ	説明
Host <i>{string}</i>	<p>接続するActive Directoryサービスのサーバーが稼働しているホストのドメイン名 (FQDN) または IP アドレス。</p> <p>例 : "win2012.win.local"</p> <p>デフォルト値 : (未設定)</p>
Port <i>{integer}</i>	<p>Active Directoryサービスのサーバーがリッスンするホスト上のポート。</p> <p>デフォルト値 : 389</p>
Dn <i>{string}</i>	<p>Active Directory内のオブジェクトのDN。これはLDAP URLのdn部分に似ています。</p> <p>例 : "dc=win,dc=local"</p> <p>デフォルト値 : (未設定)</p>
User <i>{string}</i>	<p>識別に使用される、サーバー上のユーザーID。</p> <p>例 : "Administrator@WIN.LOCAL"</p> <p>デフォルト値 : (未設定)</p>
Password <i>{string}</i>	<p>Active Directoryサーバー上での認証に使用されるユーザーのパスワード。</p> <p>デフォルト値 : (未設定)</p>
ChaseReferrals <i>{Boolean}</i>	<p>現在のActive Directoryサーバーがリクエストへの応答として他のLDAPサーバーへの参照を返す場合、その参照に従うようコンポーネントに指示します。</p> <p>デフォルト値 : No</p>



UseSSL <i>{Boolean}</i>	Active Directoryサーバーへの接続にSSL/TLSを使用するよう指示します。 デフォルト値 : No
----------------------------	--

3. AllMatch、Mask、Regex、Cidrタイプのセクションパラメータ

パラメータ	説明
File <i>{path}</i>	検索文字列を含むテキストファイルへのパス。 例 : "/etc/file1" デフォルト値 : (未設定)

機能

- AllMatchタイプのセクションで指定したファイルの文字列は、大文字と小文字を区別しない完全に一致する文字列の検索に使用されます。
- Maskタイプのセクションで指定したファイルの文字列は、マスク(ワイルドカード)と見なされます。マスクは、標準文字と特殊文字を含む正規表現の簡略版と見なすことができます。文字列とマスクの照合は、大文字と小文字を区別しないで行われます。マスクには、次の特殊文字と式を含めることができます。

* - 任意の文字シーケンス

? - 任意の1つの記号

[<character set>] - セットの文字(たとえば、[bac])

[<character set>] - セットのどの記号にも一致しない文字(たとえば、[!cab])

[[: <class>:]] - 文字 (*alnum*、*alpha*、*ascii*、*blank*、*cntrl*、*digit*、*graph*、*lower*、*print*、*punct*、*space*、*upper*、*xdigit*) のPOSIXクラスの文字

サブストリングと一致するマスクには、「*」記号で囲まれたサブストリングが含まれている必要があります。(例: *host*)。いずれかの特殊文字を指定する必要がある場合は、バックスラッシュを使用して文字をエスケープする必要があります(\\[、\\]、*、\\?)。必要に応じて、バックスラッシュをエスケープすることもできます(\\)。他の文字をエスケープしても意味はありません。たとえば文字列\\a\\b\\c*\\d\\?\\は文字列abc*d?\\に変換されます。マスクの例:



```
#Matches the "name" string exactly
name

#Matches the three-character strings where
#the first character is "c", the second is any, and the third is "t"
#For example: "cat", "cut", "cct"
c?t

#Matches the strings: "user", "users", "us3rr", "ussrl", and so on
#(the [:alpha:] character class matches any alphabetical
#character, the special character "?" matches any character)
us[[:alpha:]]34)r?

#Matches the strings: ".con", "file.col", "3...co!", and so on
#(any character sequence before the ".co", after-
#any character except "m" and "?")
*.co[!m\?]
```

```
#Matches any string that contains "host",
#For example: "host", "localhost", "hostel", "ghosts"
*host*
```

- **Regex**タイプのセクションで指定したファイルの文字列は、PCRE (*Perl互換正規表現*) の通常の拡張機能として解釈されます。文字列と正規表現の照合は、大文字と小文字を区別しないで行われます。正規表現の例:

```
#IPv4
(\d{1,3}\.){3}\d{1,3}

#Email address in the .com domain
\w+@\w+\.com
```

- **Cidr**タイプのセクションで指定したファイルの文字列は、IPアドレスまたはIPアドレス範囲として解釈されます。IPアドレスとIPアドレス範囲では、IPv4形式とIPv6形式が許可されます。サブネットマスクは、ビット (オクテット) 形式とCIDR (*Classless Inter-Domain Routing*) 表記で指定できます。例:

```
#IPv4
192.168.0.1
192.168.0.0/12
192.168.0.0/255.255.255.224

#IPv6
fe80::c7e8/32
fe80::c7e8/255.255.255.224
```

4. Pq、Mysql、Sqliteタイプのセクションで使用されるパラメータ

<p>Conn</p> <p><i>{string}</i></p>	<p>データベース接続文字列。</p> <p>使用可能な値:</p> <ul style="list-style-type: none"> • Mysql (MySQL)、Pq (PostgreSQL) セクションの場合: <pre>tcp://[<user>[:<password>]@]<host>[:<port>][/] <database name>][?<parameter>=<value>[&...]]</pre>
------------------------------------	--



	<p>unix://[<user>[: <password>]@]<path to socket>[: <database name>][? <parameter>=<value>[&...]]</p> <p>例: "tcp://user:pwd@localhost:1234/userdb", "unix://user:pwd@/tmp/pgsql.sock:userdb"</p> <p>URI要件に注意してください。</p> <ul style="list-style-type: none"> • Sqlite(SQLite) セクションの場合: データベースファイルへのパス(file://スキームプレフィックスを指定)。 例: "file:///home/user/users.db" <p>デフォルト値: 対応する*DefaultConnパラメータ値によって定義</p>
Request <i>{string}</i>	<p>データベースへのSQLクエリ文字列(SELECT)。ADおよびLDAPタイプのソースについては、以下の自動的に許可されるマーカーをクエリで使用できます。</p> <ul style="list-style-type: none"> • \$u、\$Uは、クライアントコンポーネントによって送信されたユーザー名(user)に自動的に置き換えられます。 • \$d、\$Dは、クライアントコンポーネントによって送信されたドメイン(domain)に自動的に置き換えられます。 • \$\$は、「\$」文字に置き換えられます。 <p>例: "SELECT username FROM users INNER JOIN domains ON users.domain = domains.id WHERE domains.name = \$d AND users.name = \$u"</p> <p>デフォルト値: (未設定)</p>



SQLクエリとして、SELECTタイプのクエリのみ指定できます。置換を実行した後、クエリは「そのまま」データベースに送信されます。クエリ結果に複数のカラムが含まれる場合、最初のカラムを除くすべてのカラムが無視されます。

5. Redisタイプのセクションで使用されるパラメータ

Conn <i>{string}</i>	<p>Redisデータストレージとの接続文字列。</p> <p>使用可能な値:</p> <ul style="list-style-type: none"> • tcp://[<password>@] <host>[: <port>] [/ <database index>] • unix://[<password>@] <socket path>[: <database index>] <p>URI要件に注意してください。</p> <p>例: "tcp://localhost:6379"</p> <p>デフォルト値: RedisDefaultConnパラメータ値によって定義</p>
Request <i>{string}</i>	<p>Redisストレージのクエリ文字列。クエリでは、以下の自動的に許可されるマーカーを使用できます。</p> <ul style="list-style-type: none"> • \$u、\$Uは、クライアントコンポーネントによって送信されたユーザー名(user)に自動的に置き換えられます。 • \$d、\$Dは、クライアントコンポーネントによって送信されたドメイン(domain)に自動的に置き換えられます。



- \$\$は、「\$」文字に置き換えられます。

例："HVALS bad_users"

デフォルト値：(未設定)



クエリー結果に複数のカラムが含まれる場合、最初のカラムを除くすべてのカラムが無視されません。

新しいデータソース用のセクションの追加

Dr.Web for UNIX Internet Gateways用のコマンドラインベース管理ツール[Dr.Web Ctl](#)(`drweb-ctl`コマンドでアクセス)を使用し、`<name>`タグを使って、サポートされるタイプの新しいデータソース用に新しいセクションを追加するには、次のコマンドを使用する必要があります。

```
# drweb-ctl cfset LookupD.<type> -a <name>
```

例:

```
# drweb-ctl cfset LookupD.AD -a WinAD1
# drweb-ctl cfset LookupD.AD.WinAD1.Host 192.168.0.20
```

最初のコマンドは[LookupD.AD.WinAD1]という名前のセクションを設定ファイルに追加し、2番目のコマンドはこのセクション内のHostパラメータの値を変更します。

あるいは次の例のように、新しいセクションを設定ファイルの末尾に直接書き込むこともできます。

```
[LookupD.AD.WinAD1]
Host = 192.168.0.20
```



どちらの方法でも効果は同じです。ただし設定ファイルを編集する場合は、`drweb-configd`コンポーネントにSIGHUP信号を送信して、変更した設定を適用する必要があります。これを行うには、次のコマンドを実行します。

```
# drweb-ctl reload
```



Dr.Web StatD

Dr.Web StatDコンポーネントは、Dr.Web for UNIX Internet Gatewaysのコンポーネントの動作中に発生するイベントの統計を蓄積するために設計されています。イベントは永続的なリポジトリに保存され、リクエストに応じて取得できます。

動作原理

このコンポーネントは、Dr.Web for UNIX Internet Gatewaysコンポーネントの操作中に取得されたイベントの蓄積と無期限の保存を確保します。次のタイプのイベントがログに記録されます。

- コンポーネントの緊急シャットダウン
- 脅威の検出(特にメールメッセージ)

Dr.Web StatDはデーモンモードで動作し、設定制御デーモンによって自動的に起動されます。イベントの表示と管理は[Dr.Web Ct](#)ユーティリティのeventsコマンドによって確認できます。

コマンドライン引数

Dr.Web StatDを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-statd [<parameters>]
```

Dr.Web StatDは次のオプションを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了します。 短縮形：-h 引数：なし
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了します。 短縮形：-v 引数：なし

例：

```
$ /opt/drweb.com/bin/drweb-statd --help
```

このコマンドは、Dr.Web StatDに関する簡単なヘルプ情報を出力します。

スタートアップノート

このコンポーネントは、自律モードで(他のコンポーネントから自律的に)OSのコマンドラインから直接起動することはできません。必要に応じて[Dr.Web ConfigD](#)設定デーモンによって自動的に起動されます。コンポーネントの



動作を管理するには、Dr.Web for UNIX Internet Gateways用のコマンドラインベース管理ツール[Dr.Web Ctl](#)を使用できます（これはdrweb-ctlコマンドを使用して呼び出されます）。



コマンドラインから製品のこのコンポーネントに関するドキュメントを要求するには、`man 1 drweb-statd`コマンドを使用します。

設定パラメータ

このコンポーネントは、Dr.Web for UNIX Internet Gatewaysの統合された[設定ファイル](#)の[StatD]セクションで指定されている設定パラメータを使用します。

セクションには以下のパラメータが含まれています。

パラメータ	説明
LogLevel <i>{logging level}</i>	コンポーネントの ロギングレベル 。 パラメータの値が指定されていない場合は、[Root] セクション のDefaultLogLevelパラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントのファイルへの実行パス。 デフォルト値: <opt_dir>/bin/drweb-statd <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-statd• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-statd
RunAsUser <i>{UID user name}</i>	その権限によりコンポーネントを実行するユーザーの名前。このユーザー名は、ユーザーのUIDまたはユーザーのログインとして指定できます。ユーザー名が数字で構成されている場合（つまりUIDに似ている場合は）、「name:」というプレフィックスを付けて指定します。たとえば、RunAsUser = name:123456です。 ユーザー名が指定されていない場合、コンポーネント操作は開始後にエラーが発生して終了します。 デフォルト値: drweb
IdleTimeLimit <i>{time interval}</i>	コンポーネントの最大アイドル時間。指定された時間が経過すると、コンポーネントはシャットダウンします。 指定可能な値: 10秒 (10s) から30日 (30d) まで。 None値が設定されている場合、コンポーネントは永続的に機能します。コンポーネントがアイドル状態になると、SIGTERMシグナルは送信されません。 デフォルト値: 30s



パラメータ	説明
MaxEventStoreSize <i>{size}</i>	イベントデータベースの最大許容サイズ。mbで定義されます。例： MaxEventStoreSize = 100mb。 最小値：50mb デフォルト値：1GB



付録

付録A. コンピューター脅威の種類

本マニュアルでは、コンピューターやネットワークに対して潜在的または直接的な損害を与え、ユーザーの情報や権限を侵害するあらゆる種類のソフトウェアを「脅威」と定義します（悪意のあるソフトウェアやその他の不要なソフトウェア）。広義では、コンピューターまたはネットワークのセキュリティに対するあらゆる種類の潜在的な危険（すなわちハッカー攻撃につながる脆弱性）を指して「脅威」とする場合があります。

以下に記載するすべての種類のプログラムは、ユーザーのデータまたは機密情報を危険にさらすものです。姿を隠さないプログラム（スパム配信ソフトウェアやさまざまなトラフィックアナライザなど）は、状況によっては脅威と化す可能性はありますが、通常はコンピューター脅威と見なされません。

コンピューターウイルス

この種類のコンピューター脅威は、他のプログラム内にそのコードを埋め込む（これを感染と呼びます）ことができるという特徴を持っています。多くの場合、感染したファイルはそれ自体がウイルスのキャリアとなり、また埋め込まれたコードは必ずしもオリジナルのものとは一致するとは限りません。ほとんどのウイルスは、システム内のデータを破壊させる、または破壊する目的を持っています。

Doctor Webの分類では、ウイルスは感染させるオブジェクトの種類に応じて分けられます。

- **ファイルウイルス**は、OSのファイル（通常、実行ファイルおよびダイナミックライブラリ）を感染させ、そのファイルの起動と同時にアクティブになります。
- **マクロウイルス**は、Microsoft® Officeやマクロコマンドをサポートする他のアプリケーション（Visual Basicで書かれたものなど）が使用するドキュメントに感染するウイルスです。マクロコマンドは、完全に機能するプログラミング言語で書かれた一種の実装プログラム（マクロ）です。たとえば、Microsoft® Wordでは、文書を開くか、閉じるか、保存すると、マクロが自動的に開始されることがあります。
- **スクリプトウイルス**はスクリプト言語を使用して作成され、他のスクリプト（OSのサービスファイルなど）に感染します。これらはスクリプトを実行できる他のファイル形式に感染することができるため、Webアプリケーションのスクリプトの脆弱性を利用します。
- **ブートウイルス**は、ディスクやパーティションのブートレコード、またはハードドライブのマスターブートレコードに感染します。多くのメモリを必要とせず、システムのロールアウト、再起動、またはシャットダウンが実行されるまでタスクを実行し続けられます。

多くのウイルスは検出に対抗する何らかの手段を持ち、その手法は常時改良され続けていますが、それを打開する方法も常に開発されています。すべてのウイルスは、その使用する手法に応じて分類できます。

- **暗号化ウイルス**は、感染するたびにコードを暗号化して、ファイル、ブートセクター、またはメモリ内での検出を妨げます。このようなウイルスのすべてのコピーには、ウイルスのシグネチャとして使用される可能性がある小さな共通コードの一部（復号手順）しか含まれていません。
- **ポリモーフィック型ウイルス**も同様に自身のコードを暗号化しますが、ウイルスのコピーごとに異なる特別な復号プロシージャの生成も行います。つまり、この種のウイルスにはシグネチャバイトがありません。
- **ステルスウイルス**は、特定のアクションを実行して、感染したオブジェクトでの活動と存在を隠します。このようなウイルスは、オブジェクトを感染させる前にそのオブジェクトの特性を収集し、スキャナが変更されたファイルを探し出す際に誤認させるための「ダミー」特性を作り出します。



ウイルスは、書かれているプログラミング言語（ほとんどの場合アセンブラ、高級プログラミング言語、スクリプト言語など）、または感染させるOSに応じて分類することもできます。

コンピューターワーム

「コンピューターワーム」型の悪意のあるプログラムは、ウイルスやその他のマルウェアよりも多く見られるようになってきています。ウイルス同様、自身を複製し拡散できますが、他のオブジェクトを感染させることはありません。ネットワークを通じて（通常、メールの添付ファイルとして、またはインターネットから）侵入し、ネットワーク内にある他のコンピューターにコピーを拡散します。ユーザーのアクションに応じて、または攻撃するコンピューターを選択する自動モードで拡散を開始します。

ワームは1つのファイル（ワームの本体）のみで構成されているとは限りません。多くのワームが、メインメモリ（RAM）内に読み込んだ後にワームの本体を実行ファイルとしてネットワーク経由でダウンロードする感染部分（シェルコード）を持っています。シェルコードがシステム内に存在するだけであれば、システムを再起動することで（RAMが削除されリセットされます）ワームを削除できますが、ワームの本体がコンピューターに侵入してしまった場合はアンチウイルスプログラムのみが対処可能です。

ワームはその驚異的な拡散速度によって、ペイロードを持っていない（直接的な被害を与えない）場合であっても、ネットワーク全体の機能を破壊する能力を持っています。

Doctor Webの分類では、ワームはその拡散方法によって以下のように分けられます。

- ネットワークワームは、さまざまなネットワークとファイル共有プロトコル経由で自身のコピーを拡散します。
- メールワームは、メールプロトコル（POP3、SMTPなど）を使用して拡散します。
- チャットワームは、広く使用されているメッセージングやチャットプログラム（ICQ、IM、IRCなど）のプロトコルを使用します。

トロイの木馬プログラム（トロイの木馬）

この種類のコンピューター脅威は自身を複製しません。トロイの木馬は頻繁に使用されるプログラムに成り代わり、その機能を実行します（または動作を模倣します）。同時に、システム内で悪意のあるアクション（データの破損または破壊、機密情報の送信など）を実行したり、ハッカーが許可なしにコンピューターにアクセス（たとえば第三者のコンピューターに損害を与えるために）したりすることを可能にします。

トロイの木馬の悪意のある機能は、ウイルスのそれに似ています。トロイの木馬は、ウイルスのコンポーネントである場合もあります。しかし、ほとんどのトロイの木馬は、ユーザーまたはシステムタスクによって起動される個別の実行ファイルとして配布されます（ファイル交換サーバー、リムーバブルストレージ、メール添付ファイルなどを介して）。

トロイの木馬は、よくウイルスやワームによって拡散されることや、他の種類の脅威によっても実行されうる、悪意のあるアクションの多くがトロイの木馬にも起因することから、その分類が難しくなっています。以下のトロイの木馬は、Doctor Webでは個別のクラスとして分類されています。

- バックドアは、侵入者がシステムにログオンしたり、既存のアクセスやセキュリティ対策を回避する特権機能を取得したりすることを可能にするトロイの木馬です。バックドアはファイルに感染しませんが、レジストリキーを変更して自身をレジストリに書き込みます。
- ルートキットは、自身を隠すためにOSのシステム機能を監視する際に使用されます。さらに、ルートキットは、他のプログラム（他の脅威）、レジストリキー、フォルダ、ファイルのプロセスを隠すことができます。ルートキットは独立したプログラムとして、または別の悪意のあるプログラムのコンポーネントとして拡散されます。動作モードに応じて2種類のルートキットがあります。ユーザーモードで動作（ユーザーモードライブラリの機能を監視）する



ユーザーモードのルートキット(UMR)とカーネルモードで動作する(システムのカーネルレベルで機能を監視して、悪意のあるプログラムを検出しにくくする)カーネルモードのルートキット(KMR)。

- キーロガーは、ユーザーがキーボードを使って入力したデータを記録するために使用されます。目的は、個人情報(ネットワークパスワード、ログイン、クレジットカードデータなど)を盗むことです。
- クリッカーは、Webサイトのトラフィックを増加させる目的で、またはDDoS攻撃を実行するためにハイパーリンクを別の(ときに有害な)アドレスにリダイレクトします。
- プロキシ型トロイの木馬は被害者のコンピューターを介して匿名でインターネットにアクセスします。

トロイの木馬は、Webブラウザのスタートページを変更したり特定のファイルを削除したりするなど、上記以外の悪意のあるアクションも実行することがあります。ただしそのような動作は、他の種類の脅威(ウイルスやワーム)によって実行される場合もあります。

ハッキングツール

ハッキングツールは、侵入者によるハッキングを可能にするプログラムです。最も一般的なものは、ファイアウォールまたはその他のコンピューター保護システムコンポーネントの脆弱性を検出するポートスキャナです。それらのツールはハッカーだけではなく、管理者がネットワークのセキュリティを検査するためにも用いられます。ハッキングに使用することのできる一般的なソフトウェアや、ソーシャルエンジニアリングテクニックを使用するさまざまなプログラムもハッキングツールに含まれることがあります。

アドウェア

通常、ユーザーの画面に強制的に広告を表示させるフリーウェアプログラム内に組み込まれたプログラムコードを指します。ただしそのようなコードは、他の悪意のあるプログラム経由で配布されてWebブラウザ上に広告を表示させる場合もあります。アドウェアプログラムの多くは、スパイウェアによって収集されたデータを用いています。

ジョークプログラム

アドウェア同様、この種類の軽微な脅威はシステムに対して直接的な被害を与えることはありません。ジョークプログラムは通常、実際には起こっていないエラーに関するメッセージを表示させ、データの損失につながるアクションの実行を要求します。その目的はユーザーを驚かせたり不快感を与えたりすることにあります。

ダイアラー

幅広く電話番号をスキャンし、モデムとして応答するものを見つけるための特別なコンピュータープログラムです。その後、攻撃者がその番号を使用することによって被害者に通話料の請求書が送られます。または被害者が気づかぬうちに、モデム経由で高額な電話サービスに接続されます。

リスクウェア

これらのソフトウェアアプリケーションは悪意のある目的のために作成されたものではありませんが、コンピューターセキュリティに対する脅威となりうる特徴を持っています。リスクウェアプログラムはデータを破損または削除してしまう可能性があるのみならず、クラッカー(悪意のあるハッカー)や悪意のあるプログラムによって、システムに被害を与える目的で使用されることがあります。そのようなプログラムの中には、さまざまなリモートチャットおよび管理ツール、FTPサーバーなどがあります。



疑わしいオブジェクト

ヒューリスティックアナライザによって検出される潜在的なコンピューター脅威です。これらのオブジェクトは、あらゆるタイプの脅威(ITセキュリティの専門家も把握していないもの)である可能性があり、または誤検出の場合もあります。疑わしいオブジェクトを含むファイルを隔離に移動するよう選択することをお勧めします。解析のために Doctor Web アンチウイルススラボにも送信する必要があります。



付録B. コンピューター脅威の駆除

この付録の内容

- [検出方法](#)
- [脅威に関連したアクション](#)

Doctor Webアンチウイルスソリューションは、悪意のあるソフトウェア検出に複数の手法を同時に使用します。それにより、感染が疑われるファイルに対する徹底的なスキャンを実行し、ソフトウェアの動作を管理できます。

検出方法

シグネチャ解析

スキャンはまず、ファイルコードセグメントを既知のウイルス署名と比較するシグネチャ解析で始まります。シグネチャはウイルスを特定するために必要かつ十分な、連続するバイトの有限なシーケンスです。シグネチャ辞書のサイズを抑えるため、Dr.Webアンチウイルスソリューションはシグネチャのシーケンス全体ではなくチェックサムを使用します。チェックサムはシグネチャを特定し、ウイルス検出および駆除の正確さを維持します。Dr.Webウイルスデータベースは、いくつかのエントリによって、特定のウイルスのみでなく脅威のクラス全体を検出できるよう設計されています。

Origins Tracing™

シグネチャ解析の完了後、Dr.Webアンチウイルスソリューションは既知の感染メカニズムを用いる新種・亜種ウイルスを検出するため、ユニークなテクノロジーOrigins Tracing™を使用します。それにより、Dr.WebユーザーはランサムウェアであるTrojan.Encoder.18(別名gpcode)のような悪質な脅威から保護されます。新種・亜種ウイルスの検出を可能にする他、Origins Tracing™はDr.Webヒューリスティックアナライザによる誤検出を劇的に減らします。Origins Tracing™アルゴリズムを使用して検出されたオブジェクトの名前には、.Origin拡張子が付きます。

実行のエミュレーション

プログラムコードエミュレーションの技術は、チェックサムによる検索が直接適用できない場合、または実行するのが非常に困難な場合(安全な署名を構築することが不可能なため)に、ポリモーフィック型ウイルスと暗号化ウイルスの検出に使用されます。この方法は、エミュレーター、つまりプロセッサとランタイム環境のプログラミングモデルによる解析コード実行のシミュレーションを意味します。エミュレーターは保護されたメモリ領域(エミュレーションバッファ)で動作し、解析されたプログラムの実行は命令ごとにモデル化されます。ただし、これらの命令は実際にはCPUによって実行されるものではありません。エミュレーターがポリモーフィック型ウイルスに感染したファイルを受信すると、エミュレーションの結果は復号されたウイルスコードになります。これは、シグネチャチェックサムを検索することで簡単に判別できます。

ヒューリスティック解析

ヒューリスティックアナライザの検出手法は、ウイルスコードに典型的な、または非常にまれな特徴(属性)に関する特定の情報に基づいています(ヒューリスティック)。各属性は、その深刻度および信頼度を定義する重み係数を持っています。属性が悪意のあるコードであることを示している場合には重み係数がプラスになり、コンピュー



ター脅威の特徴を示していない場合はマイナスになります。ヒューリスティックアナライザはファイルの重み付け合計値に応じて、未知のウイルスに感染している可能性を計算します。それらの合計が一定のしきい値を超えている場合、ヒューリスティックアナライザによって、オブジェクトは未知のウイルスに感染している可能性があるとして判定されます。

ヒューリスティックアナライザはファイル解凍の柔軟なアルゴリズムであるFLY-CODE™テクノロジーも使用します。このテクノロジーは、Dr.Webにとって既知のパッカーのみでなく、これまでに発見されていない未知のパッカーによって圧縮されたファイル内に悪意のあるオブジェクトが存在する可能性をヒューリスティックに検出します。Dr.Webアンチウイルスソリューションは圧縮されたオブジェクトのスキャン中に構造エントロピー解析も使用します。このテクノロジーはコードの配置を解析することで脅威を検出します。そのため、1つのウイルスデータベースから、同じポリモーフィックパッカーによって圧縮された他の多くの脅威を検出することが可能になります。

不確実な状況で仮説を扱うあらゆるシステム同様、ヒューリスティックアナライザもまたタイプIまたはタイプIIのエラーを生じさせる可能性があります（ウイルスを見逃す、または誤検知）。そのため、ヒューリスティックアナライザによって検出されたオブジェクトは「疑わしい」オブジェクトとして定義されます。

上記のスキャン手法に加え、Dr.Webアンチウイルスソリューションは既知の悪意のあるソフトウェアに関する最も新しい情報も使用します。Doctor Webアンチウイルスラボのエキスパートによって新しい脅威が発見されると、そのウイルスシグネチャ、振る舞い特性、属性を追加した更新が即座に配信されます。更新は1時間に数回行われる場合もあり、たとえ新種の悪意のあるプログラムがDr.Web常駐保護を通過してシステムに侵入した場合でも、更新後には検出され駆除されます。

クラウドベースの脅威検出テクノロジー

クラウドベースの検出方法では、あらゆるオブジェクト（ファイル、アプリケーション、ブラウザ拡張機能など）をハッシュ値によってスキャンします。ハッシュは、特定の長さの数字と文字からなる一意のシーケンスです。ハッシュ値による分析では、オブジェクトは既存のデータベースを使用してスキャンされ、カテゴリ別に分類されます（クリーン、疑わしい、悪意のある、など）。

このテクノロジーにより、ファイルスキャンの時間を最適化し、デバイスリソースを節約することができます。分析されるのはオブジェクトではなく、その固有のハッシュ値であるため、オブジェクトが悪意のあるものであるかどうかの決定はほとんど瞬時に行われます。Dr.Web Cloudサーバーに接続されていない場合、ファイルはローカルでスキャンされ、接続が復元されるとクラウドスキャンが再開されます。

Dr.Web Cloudサービスは多くのユーザーから情報を収集し、これまで未知であった脅威に関するデータを迅速に更新します。これにより、デバイス保護の効果を高めます。

アクション

コンピューター脅威を回避するために、Dr.Web製品は悪意のあるオブジェクトに対してさまざまなアクションを適用します。ユーザーはデフォルト設定を使用したり、自動的に適用するアクションを設定したり、あるいは検出のたびに手動でアクションを選択したりできます。使用可能なアクションは以下のとおりです。

- **Ignore (無視)** - いずれのアクションも実行せず、検出された脅威をスキップするように指示します。
- **Report (報告)** - 他のすべてのアクションを実行せず、検出された脅威について通知するように指示します。
- **Cure (修復)** - 感染したオブジェクトから悪意のあるコンテンツのみを削除し、修復するように指示します。ただし、すべての種類の脅威に対して適用できるわけではありません。



- **Quarantine (隔離)** - 検出された脅威を特別なディレクトリに移し、残りのシステムから隔離するように指示します。
- **Delete (削除)** - 感染したオブジェクトを永久に削除するように指示します。



コンテナ(アーカイブ、メールメッセージなど)内のファイルで脅威が検出された場合は、削除アクションの代わりにコンテナの隔離への移動が実行されます。

付録C. テクニカルサポート

Dr.Web製品のインストールまたは使用中に問題が発生した場合、テクニカルサポートへのお問い合わせの前に以下のオプションをご利用ください:

- <https://download.drweb.com/doc/> から最新のマニュアルやガイドをダウンロードして読む。
- https://support.drweb.com/show_faq/ で「よくあるご質問」を読む。
- <https://forum.drweb.com/> でDr.Webフォーラムを見る。

問題が解決しなかった場合、サポートサイト <https://support.drweb.com/> の該当するセクション内でwebフォームに必要事項を入力し、直接 Doctor Web テクニカルサポートまでお問い合わせください。

企業情報については、Doctor Web 公式サイト <https://company.drweb.com/contacts/offices/> をご覧ください。

問題に対する円滑な対応を可能にするため、テクニカルサポートにご連絡いただく前に、インストールされた製品とその設定、およびシステム環境に関するデータセットを生成することをお勧めします。これは、Dr.Web for UNIX Internet Gatewaysディストリビューションに含まれている特別なユーティリティを使用して行うことができます。

テクニカルサポートに提出するデータを収集するには、次のコマンドを使用します。

```
# <opt_dir>/bin/support-report.sh
```

<opt_dir>は、実行可能ファイルとライブラリを含むDr.Web for UNIX Internet Gatewaysファイルのディレクトリです(GNU/Linuxの場合はデフォルトで/opt/drweb.com)。ディレクトリに使用される表記規則については、[はじめに](#)を参照してください。



テクニカルサポートに提出するデータを収集する際は、ユーティリティをスーパーユーザー権限(rootユーザーの権限)で起動することをお勧めします。権限を昇格するには、suコマンドで別のユーザーとしてログインするか、sudoコマンドで別のユーザーの権限でコマンドを実行します。

ユーティリティは次の情報を収集してアーカイブします。

- OSに関するデータ(名前、アーキテクチャ、uname -aコマンドの結果)
- Doctor Webパッケージを含む、システムにインストールされているパッケージのリスト
- ログの内容:
 - Dr.Web for UNIX Internet Gatewaysのログ(コンポーネントごとに設定されている場合)
 - syslogシステムデーモンのログ(/var/log/syslog, /var/log/messages)



- システムパッケージマネージャーのログ (apt、yumなど)
- dmesgのログ
- 次のコマンドの出力: `df`、`ip a` (`ifconfig -a`)、`ldconfig -p`、`iptables-save`、`nft export xml`
- Dr.Web for UNIX Internet Gatewaysの設定と構成に関する情報:
 - ダウンロードされたウイルスデータベースのリスト (`drweb-ctl baseinfo -l`)
 - Dr.Web for UNIX Internet GatewaysディレクトリにあるファイルのリストとそれらファイルのMD5ハッシュ値
 - Dr.Web Virus-Finding EngineスキャンエンジンのバージョンとMD5ハッシュ値
 - Dr.Web for UNIX Internet Gatewaysの設定パラメータ (`drweb.ini`の内容、ルール、ルールで使用する値のファイル、Luaプロシージャなどを含む)
 - Dr.Web for UNIX Internet Gatewaysがスタンドアロンモードで動作している場合、キーファイルから取得したユーザーの情報と権限

製品とそのシステム環境に関する情報を含むアーカイブは、ユーティリティを起動したユーザーのホームディレクトリに保存されます。ファイルの名前は次のようになります。

```
drweb.report.<timestamp>.tgz
```

<timestamp>は、レポート作成時の完全なタイムスタンプ(ミリ秒単位)です(例: 20190618151718.23625)。



付録D. Dr.Web for UNIX Internet Gateways設定ファイル

すべてのDr.Web for UNIX Internet Gatewaysコンポーネントの設定パラメータは、特別な調整デーモンDr.Web ConfigDによって管理されます。これらのパラメータはdrweb.iniファイルに格納されています。デフォルトディレクトリは<etc_dir>(GNU/Linuxの場合は/etc/opt/drweb.com)です。



テキスト設定ファイルには、デフォルト値とは値の異なるパラメータのみが格納されています。パラメータが設定ファイルにない場合は、そのデフォルト値が使用されます。

<opt_dir>、<etc_dir>、<var_dir>の表記規則の詳細は、[はじめに](#)を参照してください。

設定ファイルに存在せず、かつデフォルト値を持つパラメータなど、利用可能なすべてのパラメータのリストは、次のコマンドを使用して表示できます。

```
$ drweb-ctl cfshow
```

パラメータの値は次のいずれかの方法で変更できます。

1. 設定ファイルでパラメータを指定(任意のテキストエディターでファイルを編集)し、変更を適用するためのSIGHUP信号を設定デーモン(drweb-configdコンポーネント)に送信します(これを行うには、以下のコマンドを実行します)。

```
# drweb-ctl reload
```

2. このコマンドをコマンドラインに入力します。

```
# drweb-ctl cfset <section>.<parameter> <new value>
```



このコマンドは、管理ツールDr.Web Ctlがスーパーユーザー権限で実行されている場合にのみ実行できます。スーパーユーザー権限を取得するには、suまたはsudoコマンドを使用します。

コマンドライン管理ツールDr.Web Ctl(drweb-ctlモジュール)のcfshowおよびcfsetのコマンド構文の詳細については、[Dr.Web Ctl](#)のセクションを参照してください。

ファイル構造

設定ファイルの構造は以下のとおりです。

- ファイルの内容は、名前が付けられたセクションに分割されます。こうしたセクションで利用可能な名前は厳密に事前定義されており、変更できません。セクション名は角括弧で指定され、セクションパラメータを使用するDr.Web for UNIX Internet Gatewaysコンポーネント名と似ています(設定デーモンDr.Web ConfigDのすべてのパラメータを保存する[Root]セクションは除く)。
- 設定ファイル内の「;」または「#」文字はコメントの始まりを示します。これらの文字に続くすべてのテキストは、設定パラメータの読み取り中にDr.Web for UNIX Internet Gatewaysコンポーネントによってスキップされます。
- ファイル内の各行には、次のようにパラメータ値を1つだけ含めることができます。



```
<Parameter name> = <Value>
```

- すべてのパラメータ名は厳密に事前定義されており、変更できません。
- セクション名とパラメータ名はすべて大文字と小文字が区別されません。パラメータ値も、パスに含まれるディレクトリやファイルの名前を除き (UNIX のような OS の場合)、大文字と小文字が区別されません。
- ファイル内のセクションの順序や、セクション内のパラメータの順序は重要ではありません。
- 設定ファイルのパラメータ値は引用符で囲むことができ、空白がある場合は引用符で囲む必要があります。
- 一部パラメータは複数の値を取ることができます。その場合、値はコンマで区切るか、設定ファイルの異なる行に複数指定します。前者の場合、コンマの前後の空白は無視されます。空白文字がパラメータ値の一部である場合は、その文字を引用符で囲む必要があります。

次のようにして複数の値を指定できます。

- 1) コンマ区切りのリストにする。

```
Parameter = Value1, Value2, "Value 3"
```

- 2) 設定ファイルで行を複数指定する。

```
Parameter = Value2  
Parameter = Value1  
Parameter = "Value 3"
```

値の順序は任意です。



ファイルやディレクトリへのパスをコンマで区切る場合、それらを引用符で囲む必要があります。

```
ExcludedPaths = "/etc/file1", "/etc/file2"
```

一連のパスを複数行として表す場合、引用符は必要ありません。

```
ExcludedPaths = /etc/file1  
ExcludedPaths = /etc/file2
```

- パラメータが複数の値を取り得る場合は、設定ファイルのコメントまたは本マニュアルの本文にその旨が記載されています。

設定ファイルのセクションの説明については、Dr.Web for UNIX Internet Gatewaysコンポーネントの説明を参照してください。

パラメータタイプ

設定パラメータには以下のタイプがあります。

- *address* - <IP address>:<port>として指定されたネットワーク接続アドレス。
- *boolean* - パラメータの可能な値は、YesまたはNoの2つだけです。
- *integer* - 非負の整数。
- *fractional number* - 小数部分のある非負の整数。



- *time interval* - 非負の整数と時間単位を示すサフィックス(文字)で構成される時間間隔。以下のサフィックスを使用できます。

- w - 週 (1w = 7d)
- d - 日 (1d = 24h)
- h - 時間 (1h = 60m)
- m - 分 (1m = 60s)
- s または サフィックスなし - 秒

時間間隔を秒で指定した場合、小数点の後にミリ秒を指定できます(区切り文字の後に3桁以内、0.5秒~500ミリ秒など)。異なる時間単位で複数の時間間隔を指定できます。この場合、間隔の合計が計算されます(実際には、値が設定に書き込まれる前に時間間隔は常にミリ秒に変換されます)。

基本的には、すべての時間間隔は $N_1wN_2dN_3hN_4mN_5[N_6]s$ の形式で表現されます。ここで N_1, \dots, N_6 は、この間隔に含まれる時間単位の数です。たとえば、1年(365日)は 365d、52w1d、52w24h、51w7d24h、51w7d23h60m、8760h、525600m、31536000s と表すことができます(すべてのレコードは同じ365日を表しています)。

以下の例では、30分、2秒、500ミリ秒の間隔を指定する方法を示しています。

- 1) 設定ファイルで指定する。

```
UpdateInterval = 30m2.5s
```

- 2) `drweb-ctl cfset` コマンドを使用する。

```
# drweb-ctl cfset Update.UpdateInterval 1802.5s
```

- 3) コマンドラインパラメータを使用する(例: [コマンドライン引数](#)の場合)。

```
$ drweb-se --WatchdogInterval 1802.5
```

- *size* - パラメータ値はオブジェクト(ファイル、バッファ、キャッシュなど)のサイズで表すことができ、非負の整数と、単位を表すサフィックスで構成します。以下のサフィックスを使用できます。

- mb - メガバイト (1mb = 1024kb)
- kb - キロバイト (1kb = 1024b)
- b - バイト

サフィックスを省略した場合、サイズはバイト単位と見なされます。異なる単位で複数のサイズを指定できます。この場合、サイズの合計が計算されます(実際には、サイズ値は常にバイトに変換されます)。

- *path to a directory (file)* - パラメータ値は、ディレクトリ(ファイル)へのパスである文字列になります。



ファイルパスはファイル名で終わる必要があります。



UNIX系システムでは、ディレクトリとファイルの名前は、大文字と小文字が区別されます。パラメータ記述で明示的に指定されていない場合、パスに特殊文字(?, *)のあるマスクを含めることはできません。



- *logging level* - Dr.Web for UNIX Internet Gatewaysコンポーネントのイベントを記録するレベル。以下の値を使用できます。
 - DEBUG - 最も詳細なロギングレベル。すべてのメッセージとデバッグ情報が登録されます。
 - INFO - すべてのメッセージが登録されます。
 - NOTICE - すべてのエラーメッセージ、警告、通知が登録されます。
 - WARNING - すべてのエラーメッセージと警告が登録されます。
 - ERROR - エラーメッセージのみが登録されます。
- *log type* - Dr.Web for UNIX Internet Gatewaysコンポーネントによるログの実行方法(ロギング方式)をパラメータ値で定義します。以下の値を使用できます。
 - `Stderr[:ShowTimestamp]` - メッセージは `stderr`(標準エラーストリーム)に表示されます。この値は設定デーモンの設定でのみ使用できます。バックグラウンドモードで動作する(「デーモン化される」)場合、つまりパラメータ `-d` を指定して起動した場合、バックグラウンドモードで動作するコンポーネントは端末のI/Oストリームにアクセスできないため、この値は *使用できません*。追加パラメータ `ShowTimestamp` は、すべてのメッセージにタイムスタンプを追加するように指示します。
 - `Auto` - ロギング対象のメッセージは設定デーモンDr.Web ConfigDに送られ、設定に基づいて一か所([Root]セクションのLogパラメータ)に保存されます。この値は、*設定デーモンを除く*すべてのコンポーネントに指定され、デフォルト値として使用されます。
 - `Syslog[:<facility>]` - メッセージはシステムロギングサービス `syslog` に送信されます。
 - 追加オプション `<facility>` は、`syslog` のメッセージ登録レベルを指定するために使用します。次の値を使用できます。
 - DAEMON - デーモンのメッセージ
 - USER - ユーザープロセスのメッセージ
 - MAIL - メールプログラムのメッセージ
 - LOCAL0 - ローカルプロセス0のメッセージ
 - ...
 - LOCAL7 - ローカルプロセス7のメッセージ
 - `<path>` - メッセージは指定されたログに直接保存されます。

パラメータ値の指定方法の例:

1) 設定ファイルで指定する。

```
Log = Stderr:ShowTimestamp
```

2) `drweb-ctl cfset` コマンドを使用する。

```
# drweb-ctl cfset Root.Log /var/opt/drweb.com/log/general.log
```

3) コマンドラインパラメータを使用する(例: `コマンドライン引数` の場合)。

```
$ drweb-se --Log Syslog:DAEMON
```

- *action* - 特定の脅威または別のイベントが検出されたときにDr.Web for UNIX Internet Gatewaysコンポーネントによって実行されるアクション。次の値を使用できます。
 - Report - 他のアクションは実行せず、検出された脅威についての通知のみをするよう指示します。
 - Cure - 脅威の修復を試みる(悪意のあるコンテンツのみを削除する)よう指示します。



- Quarantine - 感染したファイルを隔離に移動するよう指示します。
- Delete - 感染したファイルを削除するよう指示します。



一部のアクションは特定のイベントにのみ適用できます（たとえば「スキャンエラー」イベントではCure（修復）アクションをトリガーできません）。許可されたアクションは、常にアクションタイプのパラメータに記述されます。

他のパラメータタイプと可能な値は、パラメータの説明で指定されています。

トラフィックモニタリングのルール

このセクションの内容

- [概要](#)
- [ルールフォーマット](#)
- [条件](#)
- [アクション](#)
- [ルールで使用される変数](#)
- [不要なWebサイトと脅威のカテゴリ](#)
- [ルール条件で使用できる設定パラメータ](#)
- [設定ファイルにルールを保存する機能](#)

概要

ルールは、IF *<conditional_part>* THEN *<action_part>*などの構文で表されます。条件部分には「変数値が指定されている(いない)」または「変数値が指定セットに含まれている(いない)」のスキャンタイプが指定されます。アクション部分には一連のアクション(1つ以上)が含まれ、各アクションは最終的な解決(スキャンしたオブジェクトのスキップまたはブロック)、または「スキャンしたオブジェクトの機能の変更」、「指定変数へのセット値の割り当て」、または「指定変数の値の配列へのセット値の追加」などの修正アクションになります。

ルールで指定されているアクションは、条件部分がtrueの場合にのみ実行されます。条件部分がfalseの場合、このルールで指定されたアクションは実行されず、プログラムは次のルールにジャンプします。最終的な解決が実行されるまで、ルールは上から順に処理されます。その後、以降のルール(ある場合)はすべて無視されます。ルールを実行するときは、アクション部分のアクションを左から右に、指定された順序で実行することが重要です。アクションのチェーンに最終的な解決策があり、ルールの処理を中断する場合は、アクション部分で指定された残りのアクションは実行されません。

ルールフォーマット

ルールのフォーマットは次のとおりです。

```
[ <condition>[, <condition>[, ...]] : <action>[, <action>[, ...]]
```

ルールの条件部分(「:」の前)は省略できます。その場合、アクション部分は条件なしで実行されます。ルールの条件部分がない場合は、「:」の区切り文字を省略できます。条件部分の条件とアクション部分のアクションとの間のコンマは、論理積(「and」)の役割を果たします。条件部分は、すべての条件がtrueである場合にのみ



trueになります。アクション部分に指定されたすべてのアクションは、ルールの処理を中断する最終的な解決まで、左から右へ指定された順序で実行されます。ルールで使用されるキーワード、変数名、設定パラメータでは、大文字と小文字は区別されません。

条件

次のタイプの条件がルールで使用できます。

条件	解説
<code><variable> <value ></code>	変数の値がルールで指定された値と一致している。 同時に値のセットを含むことができる変数にのみ使用できます。
<code><variable> [not] in <set of values></code>	変数の値が、指定された値のセットに含まれている(notの場合 - 指定された値のセットと一致しない)。
<code><variable> [not] match <set of values></code>	変数の値が、指定されたセットにある任意の正規表現と一致する(notの場合 - 指定されたセットのどの表現とも一致しない)。 <div style="border: 1px solid #ccc; background-color: #e6f2e6; padding: 10px; display: inline-block;">  正規表現は、POSIX構文 (BRE, ERE) または Perl構文 (PCRE, PCRE2) のいずれかを使用して指定されます。 </div>
<code><variable> [not] gt <value></code>	変数の値が、指定された値よりも大きい(大きくない)。 単一の値を持つことができる変数にのみ使用できます。
<code><variable> [not] lt <value></code>	変数の値が、指定された値よりも小さい(小さくない)。 単一の値を持つ変数にのみ使用できます。

*) オプションのキーワードnotは否定を意味します。


変数と比較される `<set of values>` の部分は、以下の方法で指定できます。

構文	意味
<code>(<value 1>[, <value 2>[, ...]])</code>	括弧内にはチェックする値がリストされます(最小数は1以上でなければなりません)。値が1つしかなく、in条件が使用されている場合は、括弧を省略できます(場合によっては <code><variable> <value></code> になります)。



構文	意味
<code>" <section>. <parameter>"</code>	<p>設定パラメータに現在割り当てられている値のセット。引用符の間には、値（または値のセット）のチェックが必要な設定パラメータの名前を指定します（パラメータが属するセクションの名前も指定する必要があります）。</p> <p>条件として使用できるパラメータのリストは、ルールが設定されているコンポーネントによって異なります。リストは以下に示します。</p>
<code>file (" <file name>")</code>	<p>値のリストを含むテキストファイル <code><file name></code> へのパス。ファイル内の各文字列はリスト項目に対応します。先頭と末尾のスペースは無視されます。絶対パス以外は使用できません。<code><file name></code> に引用符やアポストロフィが含まれる場合、それらは <code>\'</code> でエスケープします。</p> <div data-bbox="917 801 1449 1727" style="background-color: #e6f2e6; padding: 10px;"><p> ファイルサイズは64MB未満である必要があります。</p><p>設定ファイルの読み込み中にファイルの内容が読み込まれ、ルールに挿入されます。ファイルが存在しない場合や、ファイルサイズが超過している場合は、設定の読み込み中にエラー <code>x102</code> が返されます。</p><p>Dr.Web for UNIX Internet Gatewaysの動作中にファイルを編集する場合、変更を適用するには、その内容を再度読み込む必要があります。次のコマンドを使用します。</p><pre data-bbox="1058 1406 1430 1476"># drweb-ctl reload</pre><p>ファイルからの値のセットは、すべての変数に使用できるわけではありません。ファイルからの値のセットを用いて値のスキャンに変数を使用できるかどうかは、以下に示します。</p></div>
<code><type_of_LOOKUP_request>@ <tag>[@ <value>]</code>	<p>値の配列は外部データソースからDr.Web LookupDを介して要求されます。<code><LOOKUP_query_type></code> はソースのタイプです。<code><tag></code> は、チェックされたパラメータのサンプリングのための接続を説明するセクションの名前です。オプションの <code><value></code> は、データソースから抽出された値の配列内に必要な値です。</p>



構文	意味
	<div style="border: 1px solid #ccc; padding: 10px; background-color: #e6f2e6;">  <p>Dr.Web LookupDの値は、すべての変数に使用できるわけではありません。条件の <code><scanning></code> を適用できない変数もあります。Dr.Web LookupDを使用して値をチェックできるかどうかについては、以下の各変数の説明で確認できます。</p> </div>

変数が複数の値を持つ場合は、指定された変数 `<variable>` の現在の値のセットと、指定されたセット `<set of values>` の共通集合が空でない場合に、`<variable> in <set of values>` の条件は `true` になります。

逆の場合は、`not in` の条件が `true` になります。たとえば、`x` が変数で、現在の値として `a`、`b`、`c` が設定されているとします。その場合は、

- `X in (a, b)` は、`a` と `b` の値が両方のセットにあるため、`true` になります。
- `X in (a, d, e)` は、`a` の値が両方のセットにあるため、`true` になります。
- `X in (d, e)` は、変数の値 (`a`、`b`、`c`) が (`d`、`e`) のセットにないため、`false` になります。
- `X in ()` は、変数の値の配列が空白でないため、`false` になります。
- `X not in ()` は、変数の値の配列が空白でないため、`true` になります。
- `X not in (d, e)` は、変数の値 (`a`、`b`、`c`) がセット (`d`、`e`) にないため、`true` になります。
- `X not in (a, d, e)` は、`a` が両方のセットにあるため、`false` になります。

以下の変数の説明では、各変数に値のセットを採用できるかどうかを示しています。

アクション

アクションは、オブジェクトの受け渡しを許可するかどうかを決定する **最終的な解決策** と、後続のルールを条件をチェックするときに使用できる、いくつかの変数の値を変更するアクションに分かれます。

最終的な解決

解決策	説明 (意味)
一般的な解決策	
Pass	トラフィックを通過させます (接続の作成を許可し、オブジェクトを受信者に送信します)。それ以降のルール (ある場合) は使用されません。
Block as <code><reason></code>	トラフィックをブロックします (接続の作成、または受信者へのオブジェクトの送信を禁止します)。それ以降のルール (ある場合) は使用されません。



解決策	説明（意味）
	<p>ブロックの <i><reason></i> はログに記録されます。同じ理由が、ユーザーに表示されるブラウザ通知にも使用されます。</p> <p>Blockの理由は次のとおりです。</p> <ul style="list-style-type: none"> • BlackList - ユーザーによってブラックリストに登録されているため、データをブロックします。 • <i>_match</i> - ルールの実行をトリガーするカテゴリーに属する脅威がWebリソースまたはファイルに含まれているため、ブロックします（*<i>_category</i> in (□)の条件の場合）。<i>_match</i>変数には、ブロックされたカテゴリーのリストに一致したものが含まれます。

最終的な解決策を処理する機能：

- Block as BlackListは、常に「ブラックリストに含まれる」として処理されます（ルールでこの解決策に指定された条件を考慮しません）。
- Block as *_match*は、*_match*が空白でない場合は「*_match*カテゴリーに属する」として処理されます。
- Block as *_match*は、*_match*が空白の場合は「ブラックリストに含まれる」として処理されます（ルールでこの解決策に指定された条件を考慮しません）。
- すべてのルールが考慮されていて、解決策のあるルールがいずれも実行されない（またはルールに解決策がない）場合、この状況はPassアクションと同じです。

変数の値の変更

変数値を変更するには、次の命令を使用します。

```
SET <variable> = ([<value 1>[, <value 2>[, ...]])
```

括弧内に値がない場合は、変数値のリストは消去されます。

```
SET <variable> = ()
```

変数の値が1つだけの場合、括弧は使用されません。

```
SET <variable> = <value>
```

ルールで使用される変数

変数の大文字と小文字は区別されません。複数のアクション名を持つ変数は、アンダースコアを使用しても使用しなくても書くことができます。したがって、*variable_name*、*VariableName*、*variablename*という名前は、実際には同じ名前の同等のバリエーションになります。以下の表では、すべての変数の名前はアンダースコアを使用して書かれています。



共通変数

変数	説明	使用可能	
		条件	アクション (SET)
protocol	<p>接続で使用されるネットワークプロトコル</p> <p>この変数は複数の値を取ることができます。</p> <p>使用可能な値: HTTP、SMTP、IMAP、POP3。</p> <p>使用方法</p> <ul style="list-style-type: none">• 変数値は、SSL/TLSが使用されていない場合、またはSSLのラップ解除が許可されている場合にのみ定義できます。• Dr.Web ICAPDのルールで可能な変数の値はHTTPだけです。• 変数の値をチェックするための値のセットは、テキストファイルから読み込むことができます。 <p>例:</p> <pre>protocol in (HTTP, SMTP) protocol in (POP3) protocol in file("/etc/file")</pre>	Yes	No
sni_host	<p>SSL/TLSを介して接続が確立されるSNIホスト(アドレス)。</p> <p>使用方法</p> <ul style="list-style-type: none">• SSLを使用しない場合、変数の値が定義されていないため、条件はfalseです。• Dr.Web ICAPDのルールではこの変数を使用できません(SSLを処理しないため、条件は常にfalseと評価されます)。• 変数の値をチェックするための値のセットは、テキストファイルから読み込むことができます。• この変数はproc変数と組み合わせて使用できます(以下を参照)。 <p>例:</p> <pre>sni_host not in ('vk.com', 'ya.ru') sni_host in "LinuxFirewall.BlackList" sni_host in file("/etc/file")</pre>	Yes	No



変数	説明	使用可能	
		条件	アクション (SET)
sni_category	<p>お使いのコンピューターがSSL/TLSを介して接続しようとしているホストで、ホスト(SNIヘッダーから識別される)が属するカテゴリー (AdultContentなど)のリスト(Webリソースカテゴリーのデータベースに準ずる)。</p> <p>この変数は複数の値を取ることができます。</p> <p>使用方法</p> <ul style="list-style-type: none">• SSLを使用しない場合、変数の値は定義されず、条件はfalseと評価されます。• Dr.Web ICAPDのルールではこの変数を使用できません(SSLを処理しないため、条件は常にfalseと評価されます)。• Dr.Web ICAPDのルールでは、ホストが事前に定義されたカテゴリー(「安全な」ホスト)のいずれにも属していても、not inが使用される条件はtrueになります。• Webリソースカテゴリーのデータベースがインストールされていない場合、変数はルールで使用できません(ルールの条件がtrueであるかどうかを確認しようとすると、エラーx112が発生します)。• 変数の値をチェックするための値のセットは、テキストファイルから読み込むことができます。 <p>例:</p> <pre>sni_category not in (AdultContent, Chats) sni_category in "LinuxFirewall.BlockCategory" sni_category in (FreeEmail) sni_category not in file("/etc/file")</pre>	Yes	No
url	<p>クライアントからリクエストされたURL。指定された文字列または正規表現と比較できます。</p> <p>使用方法</p> <ul style="list-style-type: none">• この変数はDr.Web ICAPDのルールでのみ使用できます。• Dr.Web LookupDを使用してこの変数の値をチェックできます。	Yes	No



変数	説明	使用可能	
		条件	アクション (SET)
	<ul style="list-style-type: none">変数の値をチェックするための値のセットは、ファイルから読み込むことができます。この変数はproc変数と組み合わせて使用できます(以下を参照)。 例: <pre>url match ("drweb.com", "example\..*", "aaa.ru/") url match "ICAPD.Adlist" url not match LDAP@BadURLs url match file("/etc/file")</pre>		
url_host	接続が確立されるURL/ホスト。 使用方法 <ul style="list-style-type: none">接続にSSL/TLSを使用していない場合、またはSSLのラップ解除が許可されている場合にのみ、この変数に値を設定できます。Dr.Web LookupDを使用してこの変数の値をチェックできます。変数の値をチェックするための値のセットは、テキストファイルから読み込むことができます。 例: <pre>url_host in ('vk.com', 'ya.ru') url_host not in "ICAPD.Whitelist" url_host in LDAP@hosts url_host not in file("/etc/file")</pre>	Yes	No
url_category	URL/ホストが属する カテゴリー のリスト。情報はカテゴリーのデータベースまたはDr.Web Cloudの応答に基づきます。 この変数は複数の値を取ることができます。 使用方法 <ul style="list-style-type: none">接続にSSL/TLSを使用していない場合、またはSSLのラップ解除が許可されている場合にのみ、この変数に値を設定できます。Dr.Web ICAPDのルールでは、URL/ホストが事前に定義されたカテゴリー(「安全な」URL/ホスト)のいずれにも属していません。	Yes	No



変数	説明	使用可能	
		条件	アクション (SET)
	<p>も、<code>not in</code>が使用される条件は <i>true</i> になります。Dr.Web Firewall for Linux (SpIDer Gate) のルールでは、この場合の条件は <i>false</i> になります。</p> <ul style="list-style-type: none">Webリソースカテゴリーのデータベースがインストールされていない場合、変数はルールで使用できません (ルールの条件が <i>true</i> であるかどうかを確認しようとすると、エラー x112 が発生します)。変数の値をチェックするための値のセットは、テキストファイルから読み込むことができます。 <p>例：</p> <pre>url_category not in (AdultContent, Chats) url_category in "LinuxFirewall.BlockCategory" url_category in (FreeEmail) url_category in file("/etc/file")</pre>		
<code>threat_category</code>	<p>転送されたデータにある、脅威が属する カテゴリー のリスト (ウイルスデータベースからの情報に準ずる)。</p> <p>この変数は、複数の値を指定することができます。</p> <p>使用方法</p> <ul style="list-style-type: none">接続にSSL/TLSを使用していない場合、またはSSLのラップ解除が許可されている場合にのみ、この変数に値を設定できます。Dr.Web ICAPDのルールでは、オブジェクトが事前に定義されたカテゴリー (「安全な」オブジェクト) のいずれの脅威を含んでいなくても、<code>not in</code>が使用される条件は <i>true</i> になります。Dr.Web Firewall for Linux (SpIDer Gate) のルールでは、この場合の条件は <i>false</i> になります。変数の値をチェックするための値のセットは、テキストファイルから読み込むことができます。 <p>例：</p> <pre>threat_category in "LinuxFirewall.BlockThreat" threat_category not in (Joke)</pre>	Yes	No



変数	説明	使用可能	
		条件	アクション (SET)
	<pre>threat_category in file("/etc/file")</pre>		
user	<p>その権限により、トラフィックを送信（または受信）しているプロセスが起動されるユーザー。</p> <p>使用方法</p> <ul style="list-style-type: none"> Dr.Web ICAPDのルールでは、プロキシサーバーで認証されたユーザーの名前が変数の値として設定されます。プロキシサーバーがユーザー認証をサポートしていない場合、変数の値は空です。 Dr.Web LookupDを使用してこの変数の値をチェックできます。ユーザーが特定のユーザーグループに属しているかどうかを調べる必要がある場合、グループのリストを返すLDAPまたはActive Directoryデータソースを使用して、必要なグループ（ユーザーがそのメンバーであるかどうかを確認するグループ）の名前を指定します。<type of the source for LookupD>@<source of groups>@<required group>の形式を使用します。Active Directory(AD@)へのリクエストはグループのリストのみを返すため、これらのリクエストでは @<required group> 部分を使用する必要があります。 変数の値をチェックするための値のセットは、テキストファイルから読み込むことができます。 <p>例：</p> <pre>user in ('user1', 'user2') user in AD@Winusergroups@Admins user in LDAP@AllowedUsers user not in file("/etc/file")</pre>	Yes	No
src_ip	<p>接続を確立しているホストのIPアドレス。</p> <p>使用方法</p> <ul style="list-style-type: none"> Dr.Web LookupDを使用してこの変数の値をチェックできます。 変数の値をチェックするための値のセットは、テキストファイルから読み込むことができます。 	Yes	No



変数	説明	使用可能	
		条件	アクション (SET)
	<p>例:</p> <pre>src_ip not in (127.0.0.1, 10.20.30.41, 198.126.10.0/24) src_ip in LDAP@AllowedAddresses src_ip not in file("/etc/file")</pre>		
proc	<p>接続を確立するプロセス(完全な実行パス)。</p> <p>使用方法</p> <ul style="list-style-type: none">• Dr.Web ICAPDのルールではこの変数を使用できません(プロセスに関する情報がコンポーネントに含まれていないため、条件は常にfalseと評価されます)。• 変数の値をチェックするための値のセットは、テキストファイルから読み込むことができます。• この変数はsni_host、url、dst_addressと組み合わせて使用できます(以下を参照)。 <p>例:</p> <pre>proc in ('/usr/bin/ls') proc not in ('/home/user/myapp', '/bin/bin1') proc in "LinuxFirewall.ExcludedProc" proc in file("/etc/file")</pre>	Yes	No
direction	<p>接続で送信されるメッセージのタイプ</p> <p>使用可能な値: request(クライアントリクエスト)、response(サーバー応答)。</p> <p>この変数は複数の値を取ることができません。matchとinタイプの条件は適用できません。</p> <p>例:</p> <pre>direction request direction not response</pre>	Yes	No
divert	接続の方向。	Yes	No



変数	説明	使用可能	
		条件	アクション (SET)
	<p>使用可能な値: <code>input</code>(受信 - ローカルホストの外部から作成/開始)、<code>output</code>(送信 - ローカルホストで作成/開始)。</p> <p>この変数は複数の値を取ることができません。<code>match</code>と<code>in</code>タイプの条件は適用できません。</p> <p>例:</p> <pre>divert input divert not output</pre>		
<code>content_type</code>	<p>接続で転送されるデータのMIMEタイプ</p> <p>使用方法</p> <ul style="list-style-type: none">• 接続にSSL/TLSを使用していない場合、またはSSLのラップ解除が許可されている場合にのみ、この変数に値を設定できます。• 式「*/*」は、任意のMIMEタイプのデータと、ヘッダーContent-TypeなしのHTTP応答に一致します。• Dr.Web LookupDを使用してこの変数の値をチェックできます。• 変数の値をチェックするための値のセットは、ファイルから読み込むことができます。 <p>例:</p> <pre>content_type in ("multipart/byteranges", "application/octet-stream") content_type not in ("text/*", "image/*") content_type not in ("audio/*") content_type in ("*/*") content_type in LDAP@BlockedContent content_type not in file("/etc/file")</pre>	Yes	No
<code>(proc, <variable>)</code>	<p>プロセスのネットワークアクティビティ。ここで、<code>proc</code>は完全なプロセス実行パス(上記を参照)で、<code><variable></code>はアクティビティのタイプを定義し、次のいずれかの値になります。</p> <ul style="list-style-type: none">• <code>sni_host</code> - SSL/TLSを介して接続が確立されるSNIホスト(アドレス)	Yes	No



変数	説明	使用可能	
		条件	アクション (SET)
	<ul style="list-style-type: none">• url - クライアントによってリクエストされた URL(上記を参照)• dst_address - プロセスが接続を確立するネットワークアドレス(<IP address>: <port>) <p>使用方法</p> <ul style="list-style-type: none">• 条件一致 ({ <Proc_reg>, <Var_reg> [, ...])でのみ使用します。ここで、<Proc_reg>はprocの正規表現で、<Var_reg>は <variable>の正規表現です。• Dr.Web ICAPDのルールではこの変数を使用できません(プロセスに関する情報がコンポーネントに含まれていないため、条件は常にfalseと評価されます)。 <p>例:</p> <pre>(proc, url) match ({"/usr/bin/wget", "www\.\ya\.*"}) (proc, dst_address) match ({"/usr/bin/.*", "192\.\168\.\1\.\d+:12345"})</pre>		
unwrap_ssl	<p>SSL/TLSを介して転送されたトラフィックがラップ解除されているかどうかを示します。</p> <p>使用可能な値: true、false。</p> <p>使用方法</p> <ul style="list-style-type: none">• この変数の値を空にすることはできません。命令 SET unwrap_ssl = ()は不可能です。• この変数は条件に使用できません。SSLのラップ解除のみ管理する必要があります(こちら側がトリガーしたブロッキングについての通知を含むWebページを表示するためなど)。• Dr.Web ICAPDのルールではこの変数を使用できません(SSLを処理しないため、変数の変更はルール処理に影響しません)。 <p>例:</p> <pre>SET unwrap_ssl = TRUE set Unwrap_SSL = false</pre>	No	Yes



変数	説明	使用可能	
		条件	アクション (SET)
http_templates_dir	<p>ブロックページのテンプレートが保存されているディレクトリへのパス</p> <p>パスが「/(スラッシュ)」で始まる場合は絶対パスになります。それ以外の記号で始まる場合は、相対パスになります。後者の場合、TemplatesDirパラメータで指定されたディレクトリに相対して指定されます。</p> <p>使用方法</p> <ul style="list-style-type: none"> • HTTP(S)プロトコルで使用できます。 <p>例:</p> <pre>SET http_templates_dir = "/etc/mytemplates" set http_templates_dir = "templates_for_my_site"</pre>	No	Yes

不要なWebサイトと脅威のカテゴリー

1. 望ましくないWebサイトのカテゴリー(変数sni_category、url_categoryでの使用)

表記規則	Webサイトのカテゴリー
InfectionSource	悪意のあるソフトウェアを含むWebサイト(「感染源」)
NotRecommended	閲覧が推奨されない、不正なWebサイト(「ソーシャルエンジニアリング」を使用しているもの)
AdultContent	ポルノまたはエロティックなコンテンツ、出会い系サイトなどを含むWebサイト
Violence	暴力行為を助長するWebサイトや、さまざまな死亡事故などに関するコンテンツを含むWebサイト
Weapons	武器および爆発物に関するWebサイトや、それらの製造に関する情報を提供しているWebサイト
Gambling	勝負事、カジノ、オークションなどのオンラインゲームへのアクセスを提供するWebサイト(賭けサイトなどを含む)
Drugs	麻薬の使用、製造または流通などを促進するWebサイト
ObsceneLanguage	(タイトルや記事などに)卑猥な表現を含むWebサイト
Chats	テキストメッセージのリアルタイム送信を提供するWebサイト
Terrorism	攻撃的なプロパガンダ、またはテロ攻撃などに関する内容を含むWebサイト。



表記規則	Webサイトのカテゴリー
FreeEmail	メールボックスの無料登録を提供するWebサイト
SocialNetworks	さまざまなソーシャルネットワークサービス（一般、仕事、企業、興味）、テーマ別出会い系Webサイト
DueToCopyrightNotice	接続先のリンクが一部の著作物（映画、音楽など）の著作権者によって定義されているWebサイト
OnlineGames	インターネットへの常時接続を使用してゲームへのアクセスを提供するWebサイト
Anonymizers	ユーザーが個人情報を隠し、ブロックされたWebリソースにアクセスできるWebサイト
CryptocurrencyMiningPool	仮想通貨マイニングのための一般的なサービスへのアクセスを提供するWebサイト
Jobs	求人情報のWebサイト

変数 `sni_category` と `url_category` の値として、ブロックを制御するパラメータの名前を使用することもできます（以下参照）。

2. 脅威のカテゴリー（変数 `threat_category` 用）

表記規則	脅威のカテゴリー
KnownVirus	既知の脅威（ウイルス）
VirusModification	既知の脅威（ウイルス）の亜種
UnknownVirus	未知の脅威、疑わしいオブジェクト
Adware	アドウェア
Dialer	ダイヤラー
Joke	ジョークプログラム
Riskware	リスクウェア
Hacktool	ハッキングツール

変数 `threat_category` の値として、ブロックを制御するパラメータの名前を使用することもできます（以下参照）。



ルール条件で使用される設定パラメータ

Dr.Web Firewall for Linuxのコンポーネントルールで使用されるパラメータ(プレフィックスLinuxFirewall.で示されます)

パラメータ	説明と使用例
Whitelist	<p>ホワイトリスト。Dr.WebのURLカテゴリーのデータベースに対象のドメインが含まれている場合でも、アクセスが許可されるドメインのリスト</p> <p>例:</p> <pre>sni_host in "LinuxFirewall.Whitelist" : Pass url_host not in "LinuxFirewall.Whitelist" : Block as _match</pre>
Blacklist	<p>ブラックリスト。アクセスがユーザー(または管理者)によってブロックされているドメインのリスト</p> <p>例:</p> <pre>sni_host in "LinuxFirewall.Blacklist" : SET Unwrap_SSL = FALSE url_host in "LinuxFirewall.Blacklist" : Block as BlackList</pre>
BlockCategory	<p>「メタパラメータ」: [LinuxFirewall]セクションでBlock*パラメータがYesに設定されているWebリソースカテゴリー(Chats、AdultContentなど)の名前のリスト</p> <p>例:</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match sni_category in "LinuxFirewall.BlockCategory" : Block as BlackList</pre>
BlockThreat	<p>「メタパラメータ」: [LinuxFirewall]セクションでBlock*パラメータがYesに設定されている脅威の種類(KnownVirus、Jokeなど)の名前のリスト</p> <p>例:</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : Block as _match</pre>
ExcludedProc	<p>トラフィックをスキャンから除外する必要がある、信頼できるプロセスのリスト</p> <p>例:</p> <pre>proc in "LinuxFirewall.ExcludedProc" : Pass</pre>



Dr.Web ICAPDのコンポーネントルールで使用されるパラメータ(プレフィックスICAPD.で示されます)

パラメータ	説明と使用例
Whitelist	ホワイトリストには、Dr.WebのURLカテゴリーのデータベースに対象のドメインが含まれている場合でも、アクセスが許可されるドメインのリストが含まれます。 例： <pre>url_host not in "ICAPD.Whitelist" : Block as BlackList</pre>
Blacklist	ブラックリストにはドメインのリストが含まれ、そのドメインへのアクセスはユーザー（または管理者）によってブロックされます。 例： <pre>url_host in "ICAPD.Blacklist" : Block as BlackList</pre>
Adlist	広告リスト。広告Webサイトを説明する正規表現のリストが含まれています。リストはユーザー（または管理者）によって定義されます。 例： <pre>url match "ICAPD.Adlist" : Block as BlackList</pre>
BlockCategory	「メタパラメータ」: [ICAPD]セクションでBlock*パラメータがYesに設定されているWebリソースカテゴリー (Chats、AdultContentなど) の名前のリスト 例： <pre>url_category in "ICAPD.BlockCategory" : Block as _match</pre>
BlockThreat	「メタパラメータ」: [ICAPD]セクションでBlock*パラメータがYesに設定されている脅威の種類 (KnownVirus、Jokeなど) の名前のリスト 例： <pre>threat_category in "ICAPD.BlockThreat" : Block as _match</pre>

設定ファイルにルールを保存する機能

- 設定ファイルのルールを使用するコンポーネントの設定セクションで、ルールはRuleSetなどの変数で保存され、それぞれが無制限のルールのセット(シーケンス)となります。さらに、各セットのルールは、最終的に解決されるまで、順次(下に向かって)考慮されます。
- 無条件のルール(条件部分のないアクションのみを含むルール)を設定ファイルに書き込む場合、空の条件部分と区切り文字「:」が追加されます。

たとえば、条件部分を含まずアクションのみで構成されている次のルール

```
Block as _match
```

は、設定ファイルには次のように書き込まれます。

```
: Block as _match
```



- アクション部分に複数のアクションセットが含まれるルールを設定ファイルに書き込む場合、アクションが一覧表示されるとおりの順序で、同じ条件部分とアクション部分からのアクション1つがあるルールのシーケンスとして書き込まれます。

たとえば、アクション部分に2つのアクションを含んでいる次のルール

```
user in ('user1', 'user2') : SET http_templates_dir = "/etc/mytemplates",
Block as _match
```

は、設定ファイルには2つのルールのシーケンスとして書き込まれます。

```
user in ('user1', 'user2') : SET http_templates_dir = "/etc/mytemplates"
user in ('user1', 'user2') : Block as _match
```

- ログインまたはルールは、条件部分で条件の離接(論理和)を許可しないため、論理和を実装するには、各ルールに離接語条件だけがある条件で一連のルールを記録する必要があります。

たとえば次の2つのルールは、「悪意のあるオブジェクトKnownVirusやTerrorismカテゴリーに該当するURLが検出された場合はブロックする」のルールと等しくなります。

```
threat_category in (KnownVirus) : Block as _match
url_category in (Terrorism) : Block as _match
```

次のレコードは同等です。 $(a \rightarrow x, b \rightarrow x)$ 、 $((a \rightarrow x) \wedge (b \rightarrow x))$ 、 $((a \vee b) \rightarrow x)$ 。

設定パラメータについては、管理ツールDr.Web Ctl(drweb-ctlモジュール)のコマンドcfshowとcfsetを使用して、RuleSetなどのパラメータの値(ルールなど)を表示、変更できます。コマンドライン管理ツールDr.Web Ctl(drweb-ctlモジュール)のcfshowとcfsetのコマンド構文の詳細については、[Dr.Web Ctl](#)のセクションを参照してください。



付録E. SSL証明書を生成する

安全なSSL/TLSデータチャネルと、HTTPS、LDAPS、SMTPSなどのアプリケーションプロトコルを使用するDr.Web for UNIX Internet Gatewaysコンポーネントの場合は、プライベートSSLキーと対応する証明書を提供する必要があります。一部のコンポーネントのキーと証明書は自動的に生成されます。それ以外の場合はDr.Web for UNIX Internet Gatewaysユーザーが作成する必要があります。すべてのコンポーネントがPEN形式の証明書を使用します。

認証局(CA)の検証証明書や署名付き証明書など、SSL/TLSを介した接続に使用されるプライベートキーと証明書を生成するには、コマンドラインユーティリティ`openssl`(OpenSSL暗号化パッケージに含まれる)を使用できます。

プライベートキーとそれに対応するSSL証明書を、CA検証証明書によって署名されたSSL証明書とともに生成するために必要な一連のアクションを検討します。

プライベートSSLキーと証明書を生成する

1. プライベートキー(RSAアルゴリズム、キーの長さは2048ビット)を生成するには、以下のコマンドを実行します。

```
$ openssl genrsa -out keyfile.key 2048
```

キーをパスワードで保護する場合は、`-des3`オプションを使用します。生成されたキーは、カレントディレクトリの`keyfile.key`ファイルにあります。

キーを表示するには、次のコマンドを使用します。

```
$ openssl rsa -noout -text -in keyfile.key
```

2. 既存のプライベートキーに基づいて指定された期間(この場合は365日)の証明書を生成するには、以下のコマンドを実行します。

```
$ openssl req -new -x509 -days 365 -key keyfile.key -out certificate.crt
```



このコマンドは、認証オブジェクトを識別するためのデータ(名前、組織など)を要求します。生成された証明書は、`certificate.crt`ファイルに置かれます。

生成された証明書の内容をスキャンするには、次のコマンドを使用します。

```
$ openssl x509 -noout -text -in certificate.crt
```

証明書を信頼済みCA証明書として登録する

1. 証明書ファイルをシステムの信頼済み証明書ディレクトリ(Debian/Ubuntuの`/etc/ssl/certs/`)に移動またはコピーします。
2. 信頼済み証明書ディレクトリに、証明書へのシンボリックリンクを作成します。リンクの名前は証明書のハッシュ値です。
3. 証明書を含むシステムのディレクトリの内容にインデックスを付け直します。



以下の例では、これら3つすべてのアクションを実行します。ここでは、現在の証明書ディレクトリが信頼済み証明書ディレクトリ/etc/ssl/certs/であり、信頼済み証明書として登録されている証明書が/home/user/ca.crtファイルにあると想定しています。

```
# cp /home/user/ca.crt ./
# ln -s ca.crt `openssl x509 -hash -noout -in ca.crt`.0
# c_rehash /etc/ssl/certs/
```

署名付き証明書を作成する

1. 既存のプライベートキーに基づいて証明書に署名するためのリクエスト (*Certificate Signing Request (CSR)*) を生成します。キーが存在しない場合は、生成します。

署名リクエストは次のコマンドで作成されます。

```
$ openssl req -new -key keyfile.key -out request.csr
```

このコマンドは、証明書を作成するコマンドと同様に、認証済みオブジェクトを識別するためのデータを要求します。このkeyfile.keyは、プライベートキーの既存のファイルです。受信したリクエストはrequest.csrファイルに保存されます。

リクエストの作成結果を確認するには、次のコマンドを使用します。

```
$ openssl req -noout -text -in request.csr
```

2. 次のコマンドを使用して、リクエストと既存のCA証明書に基づいて署名付き証明書を作成します。

```
$ openssl x509 -req -days 365 -CA ca.crt -CAkey ca.key -set_serial 01 -in request.csr -out sigcert.crt
```



署名付き証明書を作成するには、ルート証明書ca.crtとそのプライベートキーca.key (ca.crtとca.keyの代わりにcertificate.crt証明書とkeyfile.keyキーを使用することもできます。その場合、取得した証明書は自己署名されます)、署名リクエストのrequest.csrの3つのファイルが必要です。作成された署名付き証明書はsigcert.crtファイルに保存されます。

結果を確認するには、次のコマンドを使用します。

```
$ openssl x509 -noout -text -in sigcert.crt
```

作成する必要がある一意の証明書の数と同じだけこの手順を繰り返します。たとえば、スキャンクラスタ内の分散ファイルスキャンDr.Web Network Checkerのすべてのエージェントには、独自のキーと証明書が必要です。

署名付き証明書を変更する

一部のブラウザまたはメールクライアントでは、認証に使用される署名済み証明書をPKCS12形式に変更する必要があります。

次のコマンドを使用して証明書を変更できます。

```
# openssl pkcs12 -export -in sigcert.crt -out sigcert.pfx -inkey keyfile.key
```




Sigcert.crtは署名済み証明書の既存ファイルです。keyfile.keyは対応するプライベートキーのファイルです。変更した証明書はsigcert.pfxに保存されます。



付録F. 既知のエラー

この付録の内容

- [エラーを特定するための推奨事項](#)
- [エラーコード](#)
- [コードのないエラー](#)



本セクション内に記載されていないエラーが発生した場合は、[テクニカルサポート](#)までご連絡ください。その際、エラーコードと、問題を再現するための手順をお伝えください。

エラーを特定するための推奨事項

- 考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって/var/log/syslogファイルまたは/var/log/messagesファイルにあります)。また、以下の[コマンド](#)を使用することもできます。

```
# drweb-ctl log
```

- エラーを特定するために、個別のファイルにログを記録するよう設定し、ログへの広範な情報の出力を有効にすることが推奨されます。そのために、以下の[コマンド](#)を実行してください。

```
# drweb-ctl cfset Root.Log <path to log file>
# drweb-ctl cfset Root.DefaultLogLevel DEBUG
```

- デフォルトのロギング方法とログの詳細レベルに戻すには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.Log -r
# drweb-ctl cfset Root.DefaultLogLevel -r
```

エラーコード

エラーメッセージ: モニターチャンネルに関するエラー

エラーコード: x1

内部指定: EC_MONITOR_IPC_ERROR

説明: 1つまたは複数のコンポーネントが [Dr.Web ConfigD](#) 設定デーモンと接続できません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) drweb-ctl log を使用することもできます。



エラーの解決

1. 以下のコマンドを実行することで設定デーモンを再起動させてください。

```
# service drweb-configd restart
```

2. PAMの認証メカニズムがインストール、設定されていて、正常に動作していることを確認します。そうでない場合は、インストール・設定します（詳細についてはお使いのOSディストリビューション向けの管理者ガイドとマニュアルを参照してください）。
3. PAMが正常に設定されていて、設定デーモンを再起動しても問題が解決しない場合は、Dr.Web for UNIX Internet Gateways設定をデフォルトに復元してください。

これを行うには、たとえば以下のコマンドを実行するなどして、<etc_dir>/drweb.ini ファイルのコンテンツを削除します（[設定ファイル](#)のバックアップを作成することが推奨されます）。

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save  
# echo "" > /etc/opt/drweb.com/drweb.ini
```

設定ファイルのコンテンツを削除した後に設定デーモンを再起動させます。

4. 設定デーモンを起動することができない場合は、drweb-configd パッケージを再インストールしてください。

Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については [Dr.Web for UNIX Internet Gatewaysをインストールする](#) および [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#) のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *操作はすでに実行中です*

エラーコード: x2

内部指定: EC_ALREADY_IN_PROGRESS

説明: 操作はすでに実行中です。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください（デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります）。また、[コマンド](#) drweb-ctl log を使用することもできます。

エラーの解決

1. 操作が完了するまでお待ちください。必要に応じ、しばらく時間をおいて再度アクションを実行します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *操作は保留中です*

エラーコード: x3

内部指定: EC_IN_PENDING_STATE

説明: 要求された操作は保留中です。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください（デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります）。



ます)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 操作が開始されるまでお待ちください。必要に応じ、しばらく時間をおいて再度アクションを実行します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: ユーザーによって中断されました

エラーコード: x4

内部指定: EC_INTERRUPTED_BY_USER

説明: アクションはユーザーによって終了されました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって `/var/log/syslog` ファイルまたは `/var/log/messages` ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. しばらく時間をおいて再度アクションを実行します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 操作がキャンセルされました

エラーコード: x5

内部指定: EC_CANCELED

説明: アクションはキャンセルされました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって `/var/log/syslog` ファイルまたは `/var/log/messages` ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. しばらく時間をおいて再度アクションを実行します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: IPC接続が切断されました

エラーコード: x6

内部指定: EC_LINK_DISCONNECTED

説明: Dr.Web for UNIX Internet Gatewaysコンポーネントの1つとのプロセス間通信(IPC)が切断されました。長時間アイドル状態であるためにシャットダウンしたと考えられます。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって `/var/log/syslog` ファイルまたは `/var/log/messages` ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。



エラーの解決

1. 操作が完了していない場合は、しばらく時間をおいて再度操作を行ってください。そうでない場合、シャットダウンはエラーではありません。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 無効なIPCメッセージサイズです

エラーコード: x7

内部指定: EC_BAD_MESSAGE_SIZE

説明: コンポーネントのプロセス間通信 (IPC) 中に無効なサイズのメッセージを受信しました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 以下のコマンドを入力し、Dr.Web for UNIX Internet Gatewaysをリロードします。

```
# service drweb-configd restart
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 無効なIPCメッセージフォーマットです

エラーコード: x8

内部指定: EC_BAD_MESSAGE_FORMAT

説明: コンポーネントのプロセス間通信 (IPC) 中に無効なフォーマットのメッセージを受信しました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 以下のコマンドを入力し、Dr.Web for UNIX Internet Gatewaysをリロードします。

```
# service drweb-configd restart
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 準備が完了していません

エラーコード: x9

内部指定: EC_NOT_READY

説明: 必要なコンポーネントまたはデバイスがまだ初期化されていないため、要求されたアクションを実行できません。



考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. しばらく時間をおいて再度アクションを実行します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: コンポーネントがインストールされていません

エラーコード: x10

内部指定: EC_NOT_INSTALLED

説明: 必要なコンポーネントがまだインストールされていないため、必要な操作を実行できません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 必要なコンポーネントをインストールまたは再インストールしてください。コンポーネントの名前が分からない場合は、ログファイルを確認して特定してください。
2. 必要なコンポーネントをインストールまたは再インストールしても解決しない場合は、Dr.Web for UNIX Internet Gatewaysを再インストールしてください。

Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については [Dr.Web for UNIX Internet Gatewaysをインストールする](#) および [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#) のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 予期せぬIPCメッセージです

エラーコード: x11

内部指定: EC_UNEXPECTED_MESSAGE

説明: コンポーネントのプロセス間通信 (IPC) 中に予期せぬメッセージを受信しました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 以下のコマンドを入力し、Dr.Web for UNIX Internet Gatewaysをリロードします。

```
# service drweb-configd restart
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。



エラーメッセージ: *IPCプロトコル違反です*

エラーコード: x12

内部指定: EC_PROTOCOL_VIOLATION

説明: コンポーネントのプロセス間通信 (IPC) 中にプロトコル違反が発生しました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 以下のコマンドを入力し、Dr.Web for UNIX Internet Gatewaysをリロードします。

```
# service drweb-configd restart
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *サブシステムの状態が未知です*

エラーコード: x13

内部指定: EC_UNKNOWN_STATE

説明: Dr.Web for UNIX Internet Gatewaysの1つ以上のサブシステムの状態が不明であるため、必要な操作を実行できません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 操作を繰り返します。
2. 引き続きエラーが発生する場合は、以下のコマンドを実行することでDr.Web for UNIX Internet Gatewaysを再起動させてください。

```
# service drweb-configd restart
```

その後、操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *パスは絶対パスでなければなりません*

エラーコード: x20

内部指定: EC_NOT_A_DIRECTORY

説明: ファイルまたはディレクトリへの絶対パスが必要ですが、相対パスが指定されています。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。



エラーの解決

1. ファイルまたはディレクトリへのパスを絶対パスに変更します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 十分なメモリがありません

エラーコード: x21

内部指定: EC_NO_MEMORY

説明: 要求された操作を完了するのに十分なメモリがありません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) drweb-ctl log を使用することもできます。

エラーの解決

1. Dr.Web for UNIX Internet Gatewaysプロセスが使用可能なメモリのサイズを増やし(ulimit コマンドで上限を変更するなどして)、Dr.Web for UNIX Internet Gatewaysを再起動して操作を繰り返してください。



場合によっては、システムサービス systemd は指定した上限の変更を無視できます。この場合、ファイル /etc/systemd/system/drweb-configd.service.d/limits.conf を編集し(存在しない場合は作成)、変更後の制限値を指定します。たとえば、次のようになります。

```
[Service]
LimitDATA = 32767
```

systemd の利用可能な上限のリストはドキュメント man systemd.exec で確認できます。

以下のコマンドを入力し、Dr.Web for UNIX Internet Gatewaysを再起動します。

```
# service drweb-configd restart
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: I/Oエラー

エラーコード: x22

内部指定: EC_IO_ERROR

説明: 入出力(I/O)エラーが発生しました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) drweb-ctl log を使用することもできます。

エラーの解決

1. 必要なI/Oデバイスまたはファイルシステムのパーティションが使用可能であるかどうかを確認します。必要



に応じ、それをマウントして操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 指定されたファイルまたはディレクトリがありません

エラーコード: x23

内部指定: EC_NO_SUCH_ENTRY

説明: 指定された、ファイルシステムのオブジェクト(ファイルまたはディレクトリ)がありません。削除された可能性があります。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) drweb-ctl log を使用することもできます。

エラーの解決

1. パスを確認します。必要に応じ、それを変更して操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: パーミッションが拒否されました

エラーコード: x24

内部指定: EC_PERMISSION_DENIED

説明: コンポーネントは、指定されたファイルまたはディレクトリにアクセスできません。アイテムにアクセスするために必要な権限がない可能性があります。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) drweb-ctl log を使用することもできます。

エラーの解決

1. パスが正しいかどうか、また、コンポーネントが要求される権限を持っているかどうかを確認します。オブジェクトにアクセスする必要がある場合、アクセス権限を変更するか、コンポーネントの権限を昇格させます。操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: ディレクトリではありません

エラーコード: x25

内部指定: EC_NOT_A_DIRECTORY

説明: ファイルシステムの、指定されたオブジェクトがディレクトリではありません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) drweb-ctl log を使用することもできます。



エラーの解決

1. パスを確認します。正しいパスを指定して、操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: データファイルが破損しています

エラーコード: x26

内部指定: EC_NOT_A_DIRECTORY

説明: 要求されたデータが破損しています。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 操作を繰り返します。
2. 引き続きエラーが発生する場合は、以下のコマンドを実行することでDr.Web for UNIX Internet Gatewaysを再起動させてください。

```
# service drweb-configd restart
```

その後、操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: ファイルはすでに存在しています

エラーコード: x27

内部指定: EC_FILE_EXISTS

説明: 指定された場所に同じ名前のファイルがすでに存在します。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. パスを確認します。それを変更し、操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 読み取り専用ファイルシステム

エラーコード: x28

内部指定: EC_READ_ONLY_FS

説明: 変更しようとしているファイルシステムオブジェクト(ファイル、ディレクトリ、ソケット)は読み取り専用です。



考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. パスを確認します。ファイルシステムの書き込み可能なパーティションを指すようにパスを変更し、操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: ネットワークエラー

エラーコード: x29

内部指定: EC_NETWORK_ERROR

説明: ネットワークエラーが発生しました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. ネットワークが使用可能であること、ネットワーク設定が正しいことを確認します。必要に応じ、ネットワーク設定を変更し、操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: ドライブではありません

エラーコード: x30

内部指定: EC_NOT_A_DRIVE

説明: アクセスしたI/Oデバイスがドライブではありません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. ドライブ名を確認します。ドライブを指すようにパスを変更し、操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 予期せぬEOFがあります

エラーコード: x31

内部指定: EC_UNEXPECTED_EOF

説明: データの読み込み中に、予期せずファイルの終わりに達しました。



考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. ファイル名を確認します。必要に応じ、正しいファイルを指すようにパスを変更し、操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *ファイルが変更されています*

エラーコード: x32

内部指定: `EC_FILE_WAS_CHANGED`

説明: スキャン中のファイルが変更されました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 再スキャンしてください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *通常ファイルではありません*

エラーコード: x33

内部指定: `EC_NOT_A_REGULAR_FILE`

説明: アクセスされているオブジェクトは通常のファイルではありません(ディレクトリやソケットなどである可能性があります)。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. ファイル名を確認します。必要に応じ、通常のファイルを指すようにパスを変更し、操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *名前はすでに使用されています*

エラーコード: x34

内部指定: `EC_NAME_ALREADY_IN_USE`

説明: ファイルシステムに同じ名前のオブジェクトがあるため、オブジェクトを作成できません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してくだ



さい(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. パスを確認します。それを変更し、操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *ホストがオフラインです*

エラーコード: x35

内部指定: EC_HOST_OFFLINE

説明: ネットワーク経由でリモートホストにアクセスできません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 必要なホストが使用可能かどうかを確認します。必要に応じ、ホストアドレスを変更して操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *リソースの上限に達しています*

エラーコード: x36

内部指定: EC_LIMIT_REACHED

説明: 特定のリソースの使用について設定された上限に達しています。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 必要なリソースの使用可能状況を確認します。必要に応じ、このリソースの使用に関する上限を引き上げて、操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *異なるマウントポイントです*

エラーコード: x37

内部指定: EC_CROSS_DEVICE_LINK

説明: ファイルを復元できません。復元は、2つの異なるマウントポイント間でファイルを移動を行います。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してくだ



さい(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. ファイルを復元する別のパスを選択し、操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: アンパックエラー

エラーコード: x38

内部指定: EC_UNPACKING_ERROR

説明: アーカイブの展開に失敗しました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. アーカイブが破損していないことを確認します。アーカイブがパスワード保護されている場合、正しいパスワードを入力することで保護を解除し、操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: ウイルスデータベースが破損しています

エラーコード: x40

内部指定: EC_BASE_CORRUPTED

説明: ウイルスデータベースが破損しています。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. ウイルスデータベースディレクトリへのパスを確認してください。必要に応じてパスを変更します([設定ファイル](#)の [Root] [セクション](#)にある VirusBaseDir パラメータ)。
 - パスを表示および変更するには、[Webインターフェース](#)の全般設定ページに移動します(インストールされている場合)。
 - または、コマンドライン管理ツールの[コマンド](#)を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.VirusBaseDir <new path>
```



パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメイン ページで **更新** をクリックします。
- または、[コマンド](#) を実行します。

```
$ drweb-ctl update
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: サポートされていないバージョンのウイルスデータベースです

エラーコード: x41

内部指定: EC_OLD_BASE_VERSION

説明: 現在のウイルスデータベースは以前のバージョンのプログラム向けのものです。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) drweb-ctl log を使用することもできます。

エラーの解決

1. ウイルスデータベースディレクトリへのパスを確認してください。必要に応じてパスを変更します([設定ファイル](#)の [Root] [セクション](#)にある VirusBaseDir パラメータ)。
 - パスを表示および変更するには、[Webインターフェース](#)の全般設定 ページに移動します(インストールされている場合)。
 - または、コマンドライン管理ツールの[コマンド](#)を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.VirusBaseDir <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメイン ページで **更新** をクリックします。
- または、[コマンド](#) を実行します。

```
$ drweb-ctl update
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。



エラーメッセージ: ウイルスデータベースが空です

エラーコード: x42

内部指定: EC_EMPTY_BASE

説明: ウイルスデータベースが空です。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. ウイルスデータベースディレクトリへのパスを確認してください。必要に応じてパスを変更します([設定ファイル](#)の [Root] [セクション](#)にある `VirusBaseDir` パラメータ)。

- パスを表示および変更するには、[Webインターフェース](#)の全般設定ページに移動します(インストールされている場合)。
- または、コマンドライン管理ツールの[コマンド](#)を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.VirusBaseDir <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで **更新** をクリックします。
- または、[コマンド](#) を実行します。

```
$ drweb-ctl update
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: オブジェクトを修復できません

エラーコード: x43

内部指定: EC_CAN_NOT_BE_CURED

説明: 修復不可能なオブジェクトに対して修復アクションが適用されました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。



エラーの解決

1. オブジェクトに対して適用可能なアクションを選択し、操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: サポートされていないウイルスデータベースの組み合わせです

エラーコード: x44

内部指定: EC_INVALID_BASE_SET

説明: 現在のウイルスデータベースの組み合わせはサポートされていません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. ウイルスデータベースディレクトリへのパスを確認してください。必要に応じてパスを変更します([設定ファイル](#)の [Root] [セクション](#)にある VirusBaseDir パラメータ)。

- パスを表示および変更するには、[Webインターフェース](#)の全般設定ページに移動します(インストールされている場合)。
- または、コマンドライン管理ツールの[コマンド](#)を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.VirusBaseDir <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。
- または、[コマンド](#)を実行します。

```
$ drweb-ctl update
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: スキャンの上限に達しています

エラーコード: x45

内部指定: EC_SCAN_LIMIT_REACHED

説明: オブジェクトのスキャン中に、指定された上限を超えました。



考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

- 以下のいずれかの方法で、スキャンにおける上限を変更します(コンポーネント設定内で)。
 - [Webインターフェース](#)のコンポーネント設定のあるページ(インストールされている場合)を使用。
 - `drweb-ctl cfshow` および `drweb-ctl cfset` [コマンド](#) を使用。
- 設定の変更後、試みた操作を繰り返します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 認証に失敗しました

エラーコード: x47

内部指定: EC_AUTH_FAILED

説明: 認証に、無効なユーザー認証情報が使用されました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

- 必要な権限を持ったユーザーの有効な認証情報を入力してください。再度、認証を実行してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 認証に失敗しました

エラーコード: x48

内部指定: EC_NOT_AUTHORIZED

説明: ユーザーには、要求された操作を実行するための十分な権限がありません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

- 必要な権限を持ったユーザーの有効な認証情報を入力してください。再度、認証を実行してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 無効なアクセストークンです

エラーコード: x49

内部指定: EC_INVALID_TOKEN



説明 : Dr.Web for UNIX Internet Gatewaysコンポーネントの1つが、昇格された権限を必要とする操作へのアクセスを試みる際に無効な認証トークンを提示しました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 必要な権限を持ったユーザーの有効な認証情報を入力してください。再度、認証を実行してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *DBMSの一般的なエラーです*

エラーコード: x50

内部指定: EC_DB_COMMON_ERROR

説明 : Dr.Web LookupDによるDBMSサーバーへのリクエストは成功しませんでした。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

DBMSサーバーログも参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *データベースを開くことができません*

エラーコード: x51

内部指定: EC_DB_OPEN_ERROR

説明 : Dr.Web LookupDが接続しようとしているデータベースが利用できません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

DBMSサーバーログも参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *DBMSによって接続が閉じられました*

エラーコード: x52

内部指定: EC_DB_CONN_CLOSED

説明 : 接続がDBMSサーバーによって閉じられました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。



DMBSサーバーログも参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 無効な引数です

エラーコード: x60

内部指定: EC_INVALID_ARGUMENT

説明: コマンドを実行しようとした際に無効な引数を使用されました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 有効な引数を使用して、再度アクションを実行します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 無効な操作です

エラーコード: x61

内部指定: EC_INVALID_OPERATION

説明: 無効なコマンドを実行しようとする試みが検出されました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 有効なコマンドを使用して、再度アクションを実行します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: スーパーユーザー権限が必要です

エラーコード: x62

内部指定: EC_ROOT_ONLY

説明: アクションを実行するには、スーパーユーザー権限が必要です。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 権限をroot権限に昇格させ、再度アクションを実行します。権限を昇格させるには、`su` または `sudo` コマンドを使用します。



引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *集中管理モードでは許可されていません*

エラーコード: x63

内部指定: EC_STANDALONE_MODE_ONLY

説明: 要求されたアクションは、スタンドアロン [モード](#) で動作している場合のみ実行できます。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. Dr.Web for UNIX Internet Gatewaysの動作モードをスタンドアロンモードに変更し、操作を繰り返します。
2. Dr.Web for UNIX Internet Gatewaysをスタンドアロンモードに切り替えるには:
 - Webインターフェースがインストールされている場合は、[Webインターフェース](#)の集中管理の集中管理モードを有効にする チェックボックスをオフにします。
 - または、[コマンド](#) を実行します。

```
# drweb-ctl esdisconnect
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *サポートされていないOSです*

エラーコード: x64

内部指定: EC_NON_SUPPORTED_OS

説明: Dr.Web for UNIX Internet Gatewaysは、ホスト上にインストールされているOSをサポートしていません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. [システム要件](#) のリスト内に記載されているOSをインストールします。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *実装されていない機能です*

エラーコード: x65

内部指定: EC_NOT_IMPLEMENTED

説明: 1つまたは複数のコンポーネントに必要な機能が、現在のバージョンのプログラムには備わっていません。



考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. Dr.Web for UNIX Internet Gatewaysの設定をデフォルトに復元します。

そのために、たとえば以下のコマンドを実行するなどして、`<etc_dir>/drweb.ini`ファイルのコンテンツを削除します([設定ファイル](#)のバックアップを作成することが推奨されます)。

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

設定ファイルのコンテンツを削除した後に、次のコマンドを実行することでDr.Web for UNIX Internet Gatewaysを再起動させます。

```
# service drweb-configd restart
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 未知のオプションです

エラーコード: x66

内部指定: EC_UNKNOWN_SECTION

説明: [設定ファイル](#)に、未知のパラメータまたはDr.Web for UNIX Internet Gatewaysの現在のバージョンでサポートされていないパラメータが含まれています。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. いずれかのテキストエディターで `<etc_dir>/drweb.ini` ファイルを開き、無効なパラメータが含まれる行を削除します。ファイルを保存し、次のコマンドを実行することで [Dr.Web ConfigD](#) 設定デーモンを再起動させます。

```
# service drweb-configd restart
```

2. 問題が解決しない場合は、Dr.Web for UNIX Internet Gateways設定をデフォルトに戻してしてください。

そのために、たとえば以下のコマンドを実行するなどして、`<etc_dir>/drweb.ini`ファイルのコンテンツを削除します(設定ファイルのバックアップを作成することが推奨されます)：

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

設定ファイルのコンテンツを削除した後に設定デーモンを再起動させます。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。



エラーメッセージ: 未知のセクションです

エラーコード: x67

内部指定: EC_UNKNOWN_SECTION

説明: [設定ファイル](#)に、未知のセクションまたはDr.Web for UNIX Internet Gatewaysの現在のバージョンでサポートされていないセクションが含まれています。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. いずれかのテキストエディターで `<etc_dir>/drweb.ini` ファイルを開き、未知の(サポートされていない)セクションを削除します。ファイルを保存し、次のコマンドを実行することで [Dr.Web ConfigD](#) 設定デーモンを再起動させます。

```
# service drweb-configd restart
```

2. 問題が解決しない場合は、Dr.Web for UNIX Internet Gateways設定をデフォルトに戻してしてください。そのために、たとえば以下のコマンドを実行するなどして、`<etc_dir>/drweb.ini` ファイルのコンテンツを削除します(設定ファイルのバックアップを作成することが推奨されます):

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save  
# echo "" > /etc/opt/drweb.com/drweb.ini
```

設定ファイルのコンテンツを削除した後に設定デーモンを再起動させます。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 無効なオプション値です

エラーコード: x68

内部指定: EC_INVALID_OPTION_VALUE

説明: [設定ファイル](#)内の1つまたは複数のパラメータに、無効な値が含まれています。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 以下のいずれかの方法で、有効なパラメータ値を設定します。
 - [Webインターフェース](#)のコンポーネント設定のあるページ(インストールされている場合)を使用。
 - `drweb-ctl cfshow` および `drweb-ctl cfset` [コマンド](#)を使用。

当該パラメータの有効な値が分からない場合は、そのパラメータを使用するコンポーネントのヘルプファイルを参照してください。パラメータ値をデフォルト値に戻すこともできます。



- 設定ファイル `<etc_dir>/drweb.ini` を直接編集することも可能です。その場合は、いずれかのテキストエディターで設定ファイルを開き、無効なパラメータ値を含む行を見つけ、有効な値を設定してください。その後、ファイルを保存し、以下のコマンドを実行することで **Dr.Web ConfigD** 設定デーモンを再起動させます。

```
# service drweb-configd restart
```

- この手順で問題が解決しない場合は、Dr.Web for UNIX Internet Gateways設定をデフォルトに戻してください。

そのために、たとえば以下のコマンドを実行するなどして、`<etc_dir>/drweb.ini` ファイルのコンテンツを削除します（設定ファイルのバックアップを作成することが推奨されます）：

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

設定ファイルのコンテンツを削除した後に設定デーモンを再起動させます。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *無効な状態です*

エラーコード: x69

内部指定: EC_INVALID_STATE

説明: Dr.Web for UNIX Internet Gatewaysまたはコンポーネントの1が無効な状態であるため、必要な操作を完了できません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください（デフォルトでは、OSによって `/var/log/syslog` ファイルまたは `/var/log/messages` ファイルにあります）。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

- しばらく時間をおいて再度アクションを実行します。
- 引き続きエラーが発生する場合は、以下のコマンドを実行することでDr.Web for UNIX Internet Gatewaysを再起動させてください。

```
# service drweb-configd restart
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *使用可能な値は1つのみです*

エラーコード: x70

内部指定: EC_NOT_LIST_OPTION

説明: [設定ファイル](#) では、値のリストは単一値パラメータに関連付けられています。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください（デフォルトでは、OSによって `/var/log/syslog` ファイルまたは `/var/log/messages` ファイルにあります）。また、[コマンド](#) `drweb-ctl log` を使用することもできます。



エラーの解決

1. 以下のいずれかの方法で、有効なパラメータ値を設定します。
 - [Webインターフェース](#) のコンポーネント設定のあるページ(インストールされている場合)を使用。
 - `drweb-ctl cfshow` および `drweb-ctl cfset` [コマンド](#) を使用。

当該パラメータの有効な値が分からない場合は、そのパラメータを使用するコンポーネントのヘルプファイルを参照してください。パラメータ値をデフォルト値に戻すこともできます。

2. 設定ファイル `<etc_dir>/drweb.ini` を直接編集することも可能です。その場合は、いずれかのテキストエディターで設定ファイルを開き、無効なパラメータ値を含む行を見つけ、有効な値を設定してください。その後、ファイルを保存し、以下のコマンドを実行することで [Dr.Web ConfigD](#) 設定デーモンを再起動させます。

```
# service drweb-configd restart
```

3. この手順で問題が解決しない場合は、Dr.Web for UNIX Internet Gateways設定をデフォルトに戻してください。

そのために、たとえば以下のコマンドを実行するなどして、`<etc_dir>/drweb.ini` ファイルのコンテンツを削除します(設定ファイルのバックアップを作成することが推奨されます)：

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save  
# echo "" > /etc/opt/drweb.com/drweb.ini
```

設定ファイルのコンテンツを削除した後に設定デーモンを再起動させます。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 無効なタグ値です

エラーコード: x71

内部指定: EC_INVALID_TAG

説明: Dr.Web LookupDコンポーネントが連携するデータソースの名前に、正しくない、または無効な(存在しない)タグが使用されています。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって `/var/log/syslog` ファイルまたは `/var/log/messages` ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. タグのスペルが正しいかどうかを確認します。誤りを見つけた場合は、[設定ファイル](#) の該当するセクションを編集してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: レコードが見つかりません

エラーコード: x80

内部指定: EC_RECORD_NOT_FOUND

説明: 脅威のレコードがありません(他のDr.Web for UNIX Internet Gatewaysコンポーネントによってすでに処理されている可能性があります)。



考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. しばらくしてから脅威のリストを更新してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *レコードは現在処理中です*

エラーコード: x81

内部指定: EC_RECORD_BUSY

説明: レコードはすでに別のコンポーネントによって処理されています。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. しばらくしてから脅威のリストを更新してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *ファイルはすでに隔離済みです*

エラーコード: x82

内部指定: EC_RECORD_BUSY

説明: 検出された脅威を含むファイルを隔離に移動しようとした際に、ファイルがすでに隔離されていることが明らかになりました(脅威が別のコンポーネントによって処理された可能性があります)。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. しばらくしてから脅威のリストを更新してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *更新ゾーンはクラウドで提供されていません*

エラーコード: x83

内部指定: EC_NO_ZONE_IN_CLOUD

説明: Dr.Web Cloudを使用して更新しようとしたことが、失敗しました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してくだ



さい(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. しばらく時間をおいて再度アクションを実行します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *更新ゾーンはディスクで提供されません*

エラーコード: x84

内部指定: EC_NO_ZONE_ON_DISK

説明: オフラインモードでウイルスベースを更新しようとしたが、失敗しました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 更新に使用するデバイスへのパスが正しいことを確認します。
2. ベースを更新しようとするユーザーが、更新を含むディレクトリに対して必要な読み取り権限を持っていることを確認します。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *更新前にバックアップを行うことができません*

エラーコード: x89

内部指定: EC_BACKUP_FAILED

説明: 更新サーバーから更新をダウンロードする前に対象となるファイルのバックアップコピーを作成しようとする試みが失敗しました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 更新されたファイルのバックアップコピーを保存するディレクトリへのパスを確認します。必要に応じてパスを変更します([設定ファイル](#)の [Update] [セクション](#)にある BackupDir パラメータ)。
 - パスを表示および変更するには、[Webインターフェース](#)の **Updater** ページに移動します(インストールされている場合)。
 - または、コマンドライン管理ツールの [コマンド](#) を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow Update.BackupDir
```



新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Update.BackupDir <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Update.BackupDir -r
```

2. ウィルスデータベースを更新します。

- Webインターフェイスがインストールされている場合は、[Webインターフェイス](#)のメイン ページで **更新** をクリックします。
- または、[コマンド](#) を実行します。

```
$ drweb-ctl update
```

- ## 3. 引き続きエラーが発生する場合は、Dr.Web Updaterコンポーネントを実行しているアカウントのユーザーが、BackupDir で指定されたディレクトリへの書き込み権限を持っているかどうかを確認してください。このユーザーの名前は、RunAsUser パラメータで指定されます。必要に応じて、RunAsUser パラメータで指定されているユーザーを変更するか、ディレクトリのプロパティで足りない権限を付与します。

- ## 4. それでもエラーが続く場合は、drweb-update パッケージを再インストールします。

Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については [Dr.Web for UNIX Internet Gatewaysをインストールする](#) および [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#) のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 無効なDRLファイルです

エラーコード: x90

内部指定: EC_BAD_DRL_FILE

説明: 更新サーバーのリストが含まれているファイルの1つの整合性が侵害されました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) drweb-ctl log を使用することもできます。

エラーの解決

1. サーバーのリストを含むファイルへのパスを確認し、必要に応じてパスを変更します([設定ファイル](#)の [Update] [セクション](#)にある *DrDir を持つパラメータ)。
 - パスを表示および変更するには、[Webインターフェイス](#)の **Updater** ページに移動します(インストールされている場合)。
 - または、コマンドライン管理ツールの [コマンド](#) を使用することもできます。

現在のパラメータ値を表示するには、コマンドを使用します(<*DrDirPath> は、指定されたパラメータ名に置き換える必要があります。パラメータ名が不明な場合は、セクション内のパラメータ値を参照します。角括弧内のコマンド部分は省略します。

```
$ drweb-ctl cfshow Update[.<*DrDir>]
```



新しいパラメータ値を設定するには、コマンドを実行します (<*DrDir> は、指定されたパラメータ名に置き換える必要があります)。

```
# drweb-ctl cfset Update.<*DrDir> <new path>
```

パラメータ値をデフォルトに戻すには、コマンドを実行します (<*DrDir> は、指定されたパラメータ名に置き換える必要があります)。

```
# drweb-ctl cfset Update.<*DrDir> -r
```

2. ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。
- または、[コマンド](#)を実行します。

```
$ drweb-ctl update
```

3. それでもエラーが続く場合は、drweb-update パッケージを再インストールします。

Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については [Dr.Web for UNIX Internet Gatewaysをインストールする](#) および [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#) のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 無効なLSTファイルです

エラーコード: x91

内部指定: EC_BAD_LST_FILE

説明: 更新されたウイルスデータベースのリストが含まれているファイルの整合性が侵害されました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) drweb-ctl log を使用することもできます。

エラーの解決

1. しばらく時間をおいて再度ウイルスデータベースを更新します:

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。
- または、[コマンド](#)を実行します。

```
$ drweb-ctl update
```

2. それでもエラーが続く場合は、drweb-update パッケージを再インストールします。

Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については [Dr.Web for UNIX Internet Gatewaysをインストールする](#) および [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#) のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

**エラーメッセージ: 無効な圧縮ファイルです**

エラーコード: x92

内部指定: EC_BAD_LZMA_FILE

説明: 更新が含まれているダウンロードされたファイルで、整合性侵害が検出されました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. しばらく時間をおいて再度ウイルスデータベースを更新します:

- Webインターフェイスがインストールされている場合は、[Webインターフェイス](#)のメイン ページで **更新** をクリックします。
- または、[コマンド](#) を実行します。

```
$ drweb-ctl update
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。**エラーメッセージ: プロキシ認証エラーです**

エラーコード: x93

内部指定: EC_PROXY_AUTH_ERROR

説明: プログラムは、設定内で指定されたプロキシサーバーを使用して更新サーバーに接続できませんでした。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決1. プロキシサーバーへの接続に使用されているパラメータを確認します ([設定ファイル](#)の [Update] [セクション](#) の Proxy パラメータで設定されています)。

- 接続パラメータを表示および設定するには、[Webインターフェイス](#)の **Updater** ページに移動します(インストールされている場合)。
- または、コマンドライン管理ツールの[コマンド](#)を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow Update.Proxy
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Update.Proxy <new parameters>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Update.Proxy -r
```



2. ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。
- または、[コマンド](#)を実行します。

```
$ drweb-ctl update
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *使用可能な更新サーバーがありません*

エラーコード: x94

内部指定: EC_NO_UPDATE_SERVERS

説明: プログラムは、いずれの更新サーバーにも接続できませんでした。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) drweb-ctl log を使用することもできます。

エラーの解決

1. ネットワークが使用可能であるかどうかを確認します。必要に応じ、ネットワーク設定を変更します。
2. プロキシサーバーのみを使用してネットワークにアクセスできる場合は、プロキシサーバーに接続するためのパラメータを設定します([設定ファイル](#)の [Update] [セクション](#)の Proxy パラメータで設定できます)。
 - 接続パラメータを表示および設定するには、[Webインターフェース](#)の **Updater** ページに移動します(インストールされている場合)。
 - または、コマンドライン管理ツールの[コマンド](#)を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow Update.Proxy
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Update.Proxy <new parameters>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Update.Proxy -r
```

3. ネットワーク接続パラメータ(プロキシサーバーのパラメータを含む)が正しくてもエラーが発生する場合は、利用可能な更新サーバーのリストを使用していることを確認してください。使用されている更新サーバーのリストは、設定ファイルの [Update] セクションのパラメータ *Dr1Dir で表示されます。



*CustomDr1Dir パラメータが既存の正しいサーバーリストのファイルを示す場合、標準的な更新ゾーンのサーバーではなく、リスト内で指定されたサーバーが使用されます(対応する*Dr1Dir パラメータで指定されている値は無視されます)。

- 接続パラメータを表示および設定するには、[Webインターフェース](#)の **Updater** ページに移動します(インストールされている場合)。



- または、コマンドライン管理ツールの[コマンド](#)を使用することもできます。

現在のパラメータ値を表示するには、コマンドを使用します (<*DrIDir> は、指定されたパラメータ名に置き換える必要があります。パラメータ名が不明な場合は、セクション内のパラメータ値を参照します。角括弧内のコマンド部分は省略します。

```
$ drweb-ctl cfshow Update[.<*DrIDir>]
```

新しいパラメータ値を設定するには、コマンドを実行します (<*DrIDir> は、指定されたパラメータ名に置き換える必要があります)。

```
# drweb-ctl cfset Update.<*DrIDir> <new path>
```

パラメータ値をデフォルトに戻すには、コマンドを実行します (<*DrIDir> は、指定されたパラメータ名に置き換える必要があります)。

```
# drweb-ctl cfset Update.<*DrIDir> -r
```

4. ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで **更新** をクリックします。
- または、[コマンド](#) を実行します。

```
$ drweb-ctl update
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: キーファイルのフォーマットが無効です

エラーコード: x95

内部指定: EC_BAD_KEY_FORMAT

説明: キーファイルのフォーマットがサポートされていません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) drweb-ctl log を使用することもできます。

エラーの解決

1. キーファイルを持っているかどうか、また、キーファイルへのパスを確認します。キーファイルへのパスは、[設定ファイル](#)の [Root] [セクション](#)の KeyPath パラメータで指定できます。
 - キーファイルへのパスを表示および設定するには、[Webインターフェース](#)の全般設定ページに移動します(インストールされている場合)。
 - または、コマンドライン管理ツールの[コマンド](#)を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow Root.KeyPath
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.KeyPath <path to file>
```




パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.KeyPath -r
```

2. キーファイルをお持ちでない場合や、使用しているキーファイルが破損している場合は、キーファイルを購入してインストールしてください。キーファイル、購入、インストールに関する詳細については [ライセンス](#) のセクションを参照してください。
3. キーファイルをインストールするには、[Webインターフェース](#)のメインページの下部にあるライセンス有効化フォームを使用できます（インストールされている場合）。
4. また、<https://support.drweb.com/get+cabinet+link/>のユーザーのWebページ **My Dr.Web**で、現在のライセンスオプションを確認できます。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: ライセンスの有効期間が満了しています

エラーコード: x96

内部指定: EC_EXPIRED_KEY

説明: ライセンスの有効期限が切れています。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください（デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります）。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 新しいライセンスを購入して取得したキーファイルをインストールします。ライセンスの購入方法とキーファイルのインストールの詳細については、[ライセンス](#) のセクションを参照してください。
2. 購入したキーファイルをインストールするには、[Webインターフェース](#)のメインページの下部にあるライセンス有効化フォームを使用できます（インストールされている場合）。
3. また、<https://support.drweb.com/get+cabinet+link/>のユーザーのWebページ **My Dr.Web**で、現在のライセンスオプションを確認できます。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: ネットワークオペレーションがタイムアウトしました

エラーコード: x97

内部指定: EC_NETWORK_TIMEDOUT

説明: ネットワークオペレーションがタイムアウトしました（リモートホストが予期せず応答を停止したか、必要な接続に失敗した可能性があります）。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください（デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります）。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. ネットワークが使用可能であること、ネットワーク設定が正しいことを確認します。必要に応じ、ネットワーク設定を変更し、操作を繰り返します。



引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 無効なチェックサムです

エラーコード: x98

内部指定: EC_BAD_CHECKSUM

説明: 更新プログラムでダウンロードしたファイルのチェックサムが破損しています。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

- しばらく時間をおいて再度ウイルスデータベースを更新します:
 - Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで **更新** をクリックします。
 - または、[コマンド](#) を実行します。

```
$ drweb-ctl update
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 無効なトライアルライセンスです

エラーコード: x99

内部指定: EC_BAD_TRIAL_KEY

説明: デモキーファイルが無効です(別のコンピューターから受け取った場合など)。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

- 該当するコンピューターの新しい試用期間のリクエストを送信するか、新しいライセンスを購入して、受け取るキーファイルをインストールしてください。ライセンスの購入とキーファイルのインストールに関する詳細については [ライセンス](#) のセクションを参照してください。
- 購入したキーファイルをインストールするには、[Webインターフェース](#)のメインページの下部にあるライセンス有効化フォームを使用できます(インストールされている場合)。
- また、<https://support.drweb.com/get+cabinet+link/>のユーザーのWebページ **My Dr.Web**で、現在のライセンスオプションを確認できます。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: ブロックされているライセンスキーです

エラーコード: x100



内部指定: EC_BLOCKED_LICENSE

説明: 使用中のライセンスがブロックされています (Dr.Web for UNIX Internet Gatewaysの利用規約違反の可能性が有ります)。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください (デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 新しいライセンスを購入して取得したキーファイルをインストールします。ライセンスの購入方法とキーファイルのインストールの詳細については、[ライセンス](#) のセクションを参照してください。
2. 受領したキーファイルをインストールするには、[Webインターフェース](#)のメイン ページの下部にあるライセンス有効化フォームを使用できます (インストールされている場合)。
3. また、<https://support.drweb.com/get+cabinet+link/>のユーザーのWebページ **My Dr.Web**で、現在のライセンスオプションを確認できます。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 無効なライセンスです

エラーコード: x101

内部指定: EC_BAD_LICENSE

説明: ライセンスが別の製品のものであるか、Dr.Web for UNIX Internet Gatewaysコンポーネントの動作がライセンスで許可されていません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください (デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 新しいライセンスを購入して取得したキーファイルをインストールします。ライセンスの購入方法とキーファイルのインストールの詳細については、[ライセンス](#) のセクションを参照してください。
2. 受領したキーファイルをインストールするには、[Webインターフェース](#)のメイン ページの下部にあるライセンス有効化フォームを使用できます (インストールされている場合)。
3. また、<https://support.drweb.com/get+cabinet+link/>のユーザーのWebページ **My Dr.Web**で、現在のライセンスオプションを確認できます。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 無効な設定です

エラーコード: x102

内部指定: EC_BAD_CONFIG

説明: 設定が正しくないため、1つ以上のDr.Web for UNIX Internet Gatewaysコンポーネントが動作できません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください (デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。



エラーの解決

1. エラーが発生しているコンポーネントの名前が分からない場合は、ログファイルを確認して特定してください。
2. このエラーがDr.Web Firewall for Linuxによって引き起こされる場合、別のファイアウォールとの競合が発生している可能性があります。たとえば、Dr.Web Firewall for LinuxはFedora、CentOS、Red Hat Enterprise LinuxのFirewallDと競合することが確認されています（起動するたびに、FirewallDはDr.Web Firewall for Linuxで指定されるトラフィックルーティングルールを無効にします）。

このエラーを解決するには、以下のコマンドを実行することでDr.Web for UNIX Internet Gatewaysを再起動させてください。

```
# service drweb-configd restart
```

または

```
# drweb-ctl reload
```



FirewallDの動作を許可する場合、Dr.Web Firewall for LinuxのエラーはFirewallDが再起動（OSの再起動を含む）する度に繰り返し発生する可能性があります。FirewallDを無効にすることで、このエラーを解決することができます（お使いのOSに付属しているFirewallDのマニュアルを参照してください）。

3. エラーが別のコンポーネントによって発生している場合、以下のいずれかの方法によって、そのコンポーネントの設定をデフォルトに復元してください。
 - [Webインターフェース](#)のコンポーネント設定のあるページ（インストールされている場合）を使用。
 - `drweb-ctl cfshow` および `drweb-ctl cfset` [コマンド](#) を使用。
 - 手で [設定ファイル](#) を編集（コンポーネントセクションからすべてのパラメータを削除してください）。
4. この手順で問題が解決しない場合は、Dr.Web for UNIX Internet Gateways設定をデフォルトに戻してください。

そのために、たとえば以下のコマンドを実行するなどして、`<etc_dir>/drweb.ini` ファイルのコンテンツを削除します（設定ファイルのバックアップを作成することが推奨されます）：

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save  
# echo "" > /etc/opt/drweb.com/drweb.ini
```

設定ファイルのコンテンツを削除した後に、次のコマンドを実行することでDr.Web for UNIX Internet Gatewaysを再起動させます。

```
# service drweb-configd restart
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 無効な実行ファイルです

エラーコード: x104

内部指定: EC_BAD_EXECUTABLE

説明: コンポーネントの実行ファイルが破損しています。



考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. エラーが発生しているコンポーネントの名前が分からない場合は、ログファイルを確認して特定してください。
2. 以下の [コマンド](#) を実行することで (<component section> を、[設定ファイル](#) の該当するセクション名に変更します)、Dr.Web for UNIX Internet Gateways設定ファイル内でコンポーネントの実行可能パスを確認してください(コンポーネントセクションの ExePath パラメータ)。

```
$ drweb-ctl cfshow <component section>.ExePath
```

3. 以下のコマンドを実行することで (<component section> を、設定ファイルの該当するセクション名に変更します)、パスをデフォルトに復元します。

```
# drweb-ctl cfset <component section>.ExePath -r
```

4. この手順で問題が解決しない場合は、該当するコンポーネントのパッケージを再インストールしてください。

Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については [Dr.Web for UNIX Internet Gatewaysをインストールする](#) および [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#) のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: コアエンジンは使用できません

エラーコード: x105

内部指定: EC_NO_CORE_ENGINE

説明: Dr.Web Virus-Finding Engineのファイルが見つからないか、使用できません(脅威の検出に必要です)。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. `drweb32.dll` スキャンエンジンファイルへのパスを確認します。必要に応じてパスを変更します([設定ファイル](#) の [Root] [セクション](#) にある CoreEnginePath パラメータ)。
 - パスを表示および変更するには、[Webインターフェース](#)の全般設定ページに移動します(インストールされている場合)。
 - または、コマンドライン管理ツールの[コマンド](#)を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow Root.CoreEnginePath
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.CoreEnginePath <new path>
```



パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.CoreEnginePath -r
```

2. ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。
- または、[コマンド](#)を実行します。

```
$ drweb-ctl update
```

3. パスが正しく、ウイルスデータベースを更新した後もエラーが続く場合は、drweb-bases パッケージを再インストールしてください。

Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については [Dr.Web for UNIX Internet Gatewaysをインストールする](#) および [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#) のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: ウイルスデータベースがありません

エラーコード: x106

内部指定: EC_NO_VIRUS_BASES

説明: ウイルスデータベースが見つかりません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) drweb-ctl log を使用することもできます。

エラーの解決

1. ウイルスデータベースディレクトリへのパスを確認してください。必要に応じてパスを変更します([設定ファイル](#)の [Root] [セクション](#)にある VirusBaseDir パラメータ)。
 - パスを表示および変更するには、[Webインターフェース](#)の全般設定ページに移動します(インストールされている場合)。
 - または、コマンドライン管理ツールの[コマンド](#)を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.VirusBaseDir <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。



- または、[コマンド](#) を実行します。

```
$ drweb-ctl update
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: プロセスはシグナルによって中断されました

エラーコード: x107

内部指定: EC_APP_TERMINATED

説明: コンポーネントがシャットダウンしました(ユーザーコマンドによって、またはアイドル状態であるためなど)。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) drweb-ctl log を使用することもできます。

エラーの解決

1. 操作が完了していない場合は、再度開始してください。そうでない場合、シャットダウンはエラーではありません。
2. コンポーネントが度々シャットダウンする場合は、以下のいずれかの方法によって、そのコンポーネントの設定をデフォルトに復元します。
 - [Webインターフェース](#) のコンポーネント設定のあるページ(インストールされている場合)を使用。
 - drweb-ctl cfshow および drweb-ctl cfset [コマンド](#) を使用。
 - 手動で [設定ファイル](#) を編集(コンポーネントセクションからすべてのパラメータを削除してください)。
3. 問題が解決しない場合は、Dr.Web for UNIX Internet Gateways設定をデフォルトに戻してしてください。そのために、たとえば以下のコマンドを実行するなどして、<etc_dir>/drweb.ini ファイルのコンテンツを削除します(設定ファイルのバックアップを作成することが推奨されます):

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save  
# echo "" > /etc/opt/drweb.com/drweb.ini
```

設定ファイルのコンテンツを削除した後に、次のコマンドを実行することでDr.Web for UNIX Internet Gatewaysを再起動させます。

```
# service drweb-configd restart
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: 予期せぬプロセスの中断です

エラーコード: x108

内部指定: EC_APP_CRASHED

説明: 不具合によってコンポーネントがシャットダウンしました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。



ます)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. 中断された操作を繰り返します。
2. コンポーネントが度々異常にシャットダウンする場合は、以下のいずれかの方法によって、そのコンポーネントの設定をデフォルトに復元します。
 - [Webインターフェース](#) のコンポーネント設定のあるページ(インストールされている場合)を使用。
 - `drweb-ctl cfshow` および `drweb-ctl cfset` [コマンド](#) を使用。
 - 手動で [設定ファイル](#) を編集(コンポーネントセクションからすべてのパラメータを削除してください)。
3. 問題が解決しない場合は、Dr.Web for UNIX Internet Gateways設定をデフォルトに戻してしてください。そのために、たとえば以下のコマンドを実行するなどして、`<etc_dir>/drweb.ini` ファイルのコンテンツを削除します(設定ファイルのバックアップを作成することが推奨されます)：

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

設定ファイルのコンテンツを削除した後に、次のコマンドを実行することでDr.Web for UNIX Internet Gatewaysを再起動させます。

```
# service drweb-configd restart
```

4. Dr.Web for UNIX Internet Gateways設定を復元した後もエラーが続く場合は、コンポーネントパッケージを再インストールしてください。
Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については [Dr.Web for UNIX Internet Gatewaysをインストールする](#) および [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#) のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *互換性のないソフトウェアが検出されました*

エラーコード: x109

内部指定: EC_INCOMPATIBLE

説明: Dr.Web for UNIX Internet Gatewaysの1つまたは複数のコンポーネントが正しく動作できません。コンポーネントのシステムでの動作を妨げているソフトウェアがあります。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって `/var/log/syslog` ファイルまたは `/var/log/messages` ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. このエラーがSpIDer Gateによって発生した場合は、互換性のないプログラムがOSで実行されている可能性があります。このプログラムはNetFilterシステムのファイアウォールのルールを生成し、SpIDer Gateの正しい動作を妨げている可能性があります。おそらく、ShorewallまたはSuseFirewall2がシステムにインストールされています(SUSE Linux OSの場合)。NetFilterシステムのファイアウォールを設定するアプリケーションは、指定されたルールシステムの整合性をチェックし、それを書き換えることがあります。これが、このようなアプリケーションとSpIDer Gateが競合する主な原因と考えられます。



SpIDer Gateの動作に干渉しないように、互換性のないソフトウェアを再設定してください。それができない場合は、OSの起動時に読み込まれないようにソフトウェアを無効にしてください。次の手順によって、SuseFirewall2アプリケーション(SUSE Linux OS)を設定できます。

- 1) SuseFirewall2の設定ファイル(デフォルトでは /etc/sysconfig/SuSEfirewall2 ファイルです)を開きます。
- 2) 以下のラインを見つけます。

```
# Type: yesno
#
# Install NOTRACK target for interface lo in the raw table. Doing so
# speeds up packet processing on the loopback interface. This breaks
# certain firewall setups that need to e.g. redirect outgoing
# packets via custom rules on the local machine.
#
# Defaults to "yes" if not set
#
FW_LO_NOTRACK=""
```

- 3) FW_LO_NOTRACK パラメータ値に "no"を指定します:

```
FW_LO_NOTRACK="no"
```

- 4) SuseFirewall2を再起動します。

```
# rcSuSEfirewall2 restart
```



SuseFirewall2 設定に FW_LO_NOTRACK オプションがない場合は、アプリケーションを停止し、システム起動時のアプリの自動起動を無効にします。

競合アプリケーションを再設定または無効にした後、SpIDer Gateを再起動してください。

2. エラーが別のコンポーネントによって発生している場合、互換性のないソフトウェアを無効にするか、再設定し、それがDr.Web for UNIX Internet Gatewaysの動作を妨げないようにしてください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *Webリソースデータベースがありません*

エラーコード: x112

内部指定: EC_NO_DWS_BASES

説明: Webリソースカテゴリのデータベースがありません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. Webリソースカテゴリディレクトリのデータベースへのパスを確認してください。必要に応じてパスを変更します([設定ファイル](#)の[Root] [セクション](#)にあるDwsDirパラメータ)。
 - パスを表示および変更するには、[Webインターフェース](#)の全般設定ページに移動します(インストールされている場合)。



- または、コマンドライン管理ツールの [コマンド](#) を使用することもできます。
現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow Root.DwsDir
```

- 新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.DwsDir <new path>
```

- パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.DwsDir -r
```

2. Webリソースカテゴリのデータベースを更新:

- Webインターフェースがインストールされている場合は、[Webインターフェース](#) のメイン ページで **更新** をクリックします。
- または、[コマンド](#) を実行します。

```
$ drweb-ctl update
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *MeshDは使用できません*

エラーコード: x114

内部指定: EC_NO_MESH D

説明: ファイルスキャン時の負荷分散に必要な Dr.Web MeshDコンポーネントがありません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. `drweb-meshd` 実行ファイルへのパスを確認してください。必要に応じてパスを変更します ([設定ファイル](#) の [MeshD] [セクション](#) にある `ExePath` パラメータ)。

または、コマンドライン管理ツールの [コマンド](#) を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow MeshD.ExePath
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset MeshD.ExePath <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset MeshD.ExePath -r
```

2. 設定に Dr.Web MeshDコンポーネントの設定が含まれていない場合、または正しいパスを入力した後もエ



ラーが継続する場合は、drweb-meshd パッケージをインストールまたは再インストールしてください。

Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については [Dr.Web for UNIX Internet Gatewaysをインストールする](#) および [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#) のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *LookupDは使用できません*

エラーコード: x115

内部指定: EC_NO_LOOKUPD

説明: 外部ソースからデータを取得するために必要なDr.Web LookupDコンポーネントがありません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) drweb-ctl log を使用することもできます。

エラーの解決

1. drweb-lookupd 実行ファイルへのパスを確認してください。必要に応じてパスを変更します([設定ファイル](#)の [LookupD] [セクション](#)にある ExePath パラメータ)。

または、コマンドライン管理ツールの [コマンド](#) を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow LookupD.ExePath
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset LookupD.ExePath <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset LookupD.ExePath -r
```

2. 設定にDr.Web LookupDコンポーネントの設定が含まれていない場合、または正しいパスを入力した後もエラーが継続する場合は、drweb-lookupd パッケージをインストールまたは再インストールしてください。

Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については [Dr.Web for UNIX Internet Gatewaysをインストールする](#) および [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#) のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *UrlCheckは使用できません*

エラーコード: x116

内部指定: EC_NO_URL_CHECK

説明: 潜在的に危険な可能性があるカテゴリーや不要なカテゴリーに属しているURL接続をチェックするた



めに必要な、Dr.Web URL Checkerコンポーネントが見つかりません

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. `drweb-urlcheck` 実行ファイルへのパスを確認してください。必要に応じてパスを変更します(設定ファイルの [URLCheck] セクションにある `ExePath` パラメータ)。

または、コマンドライン管理ツールの [コマンド](#) を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow URLCheck.ExePath
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset URLCheck.ExePath <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset URLCheck.ExePath -r
```

2. 設定にDr.Web URL Checkerコンポーネントの設定が含まれていない場合、または正しいパスを入力した後もエラーが継続する場合は、`drweb-urlcheck` パッケージをインストールまたは再インストールしてください。

Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については [Dr.Web for UNIX Internet Gatewaysをインストールする](#) および [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#) のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *GateDは使用できません*

エラーコード: x117

内部指定: EC_NO_GATED

説明: ネットワーク接続のスキャンに必要なSpIDer Gateコンポーネントがありません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. `drweb-gated` 実行ファイルへのパスを確認してください。必要に応じてパスを変更します([設定ファイル](#)の [GateD] [セクション](#)にある `ExePath` パラメータ)。

または、コマンドライン管理ツールの [コマンド](#) を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow GateD.ExePath
```



新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset GateD.ExePath <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset GateD.ExePath -r
```

2. 設定にSpIDer Gateコンポーネントの設定が含まれていない場合、または正しいパスを入力した後もエラーが継続する場合は、drweb-gated パッケージをインストールまたは再インストールしてください。

Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については [Dr.Web for UNIX Internet Gatewaysをインストールする](#) および [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#) のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: ScanEngineは使用できません

エラーコード: x119

内部指定: EC_NO_SCAN_ENGINE

説明: 脅威の検出に必要なDr.Web Scanning Engineコンポーネントが見つからないか、起動に失敗しました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) drweb-ctl log を使用することもできます。

エラーの解決

1. drweb-se 実行ファイルへのパスを確認してください。必要に応じてパスを変更します([設定ファイル](#)の [ScanEngine] [セクション](#)にある ExePath パラメータ)。

または、コマンドライン管理ツールの [コマンド](#) を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow ScanEngine.ExePath
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset ScanEngine.ExePath <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset ScanEngine.ExePath -r
```

2. 正しいパスを入力した後もエラーが継続する場合は

- 次のコマンドを実行します。

```
$ drweb-ctl rawscan /
```

「エラー: 有効なライセンスが指定されていません」が出力された場合、有効なキーファイルがありません。Dr.Web for UNIX Internet Gatewaysを登録してライセンスを取得します。ライセンスを取得したら、[キー](#)



[ファイル](#) が使用可能かどうかを確認し、必要に応じてインストールします。

- お使いのOSにてSELinuxを有効化している場合、drweb-se モジュールに対するセキュリティポリシーを設定します（管理者マニュアルの [SELinuxのセキュリティポリシーを設定する](#) を参照してください）。

3. 設定にコンポーネントの設定が含まれていない場合、またはこれまでの手順で問題が解決しない場合は、drweb-se パッケージをインストールまたは再インストールしてください。

Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については [Dr.Web for UNIX Internet Gatewaysをインストールする](#) および [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#) のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *FileCheckは使用できません*

エラーコード: x120

内部指定: EC_NO_FILE_CHECK

説明: 脅威の検出に必要なDr.Web File Checkerコンポーネントが見つからないか、起動に失敗しました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください（デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります）。また、[コマンド](#) drweb-ctl log を使用することもできます。

エラーの解決

1. drweb-filecheck 実行ファイルへのパスを確認してください。必要に応じてパスを変更します（[設定ファイル](#)の [FileCheck] [セクション](#)にある ExePath パラメータ）。

または、コマンドライン管理ツールの [コマンド](#) を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow FileCheck.ExePath
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset FileCheck.ExePath <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset FileCheck.ExePath -r
```

2. 正しいパスを入力した後もエラーが継続する場合は

- お使いのOSにてSELinuxを有効化している場合、drweb-filecheck モジュールに対するセキュリティポリシーを設定します（管理者マニュアルの [SELinuxのセキュリティポリシーを設定する](#) を参照してください）。

3. 設定にコンポーネントの設定が含まれていない場合、またはこれまでの手順で問題が解決しない場合は、drweb-filecheck パッケージをインストールまたは再インストールしてください。

Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については [Dr.Web for UNIX Internet Gatewaysをインストールする](#) および [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#) のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。



エラーメッセージ: *ESAgentは使用できません*

エラーコード: x121

内部指定: EC_NO_ESAGENT

説明: 集中管理サーバーへの接続に必要なDr.Web ES Agentコンポーネントがありません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. `drweb-esagent` 実行ファイルへのパスを確認してください。必要に応じてパスを変更します([設定ファイル](#)の [ESAgent] [セクション](#)にある ExePath パラメータ)。

または、コマンドライン管理ツールの [コマンド](#) を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow ESAgent.ExePath
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset ESAgent.ExePath <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset ESAgent.ExePath -r
```

2. 設定にDr.Web ES Agentコンポーネントの設定が含まれていない場合、または正しいパスを入力した後もエラーが継続する場合は、`drweb-esagent` パッケージをインストールまたは再インストールしてください。

Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については [Dr.Web for UNIX Internet Gatewaysをインストールする](#) および [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#) のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *Firewallは使用できません*

エラーコード: x122

内部指定: EC_NO_FIREWALL

説明: ネットワーク接続のスキャンに必要なDr.Web Firewall for Linuxコンポーネントがありません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. `drweb-firewall` 実行ファイルへのパスを確認してください。必要に応じてパスを変更します([設定ファイル](#)の [LinuxFirewall] [セクション](#)にある ExePath パラメータ)。

または、コマンドライン管理ツールの [コマンド](#) を使用することもできます。



現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow LinuxFirewall.ExePath
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset LinuxFirewall.ExePath <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset LinuxFirewall.ExePath -r
```

2. 設定にDr.Web Firewall for Linuxコンポーネントの設定が含まれていない場合、または正しいパスを入力した後もエラーが継続する場合は、drweb-firewall パッケージをインストールまたは再インストールしてください。

Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については [Dr.Web for UNIX Internet Gatewaysをインストールする](#) および [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#) のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *NetCheckerは使用できません*

エラーコード: x123

内部指定: EC_NO_NET_CHECK

説明: ダウンロードしたファイルのスキャンに必要なDr.Web Network Checkerコンポーネントがありません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) drweb-ctl log を使用することもできます。

エラーの解決

1. drweb-netcheck 実行ファイルへのパスを確認してください。必要に応じてパスを変更します([設定ファイル](#)の[Netcheck] [セクション](#)にある ExePath パラメータ)。

または、コマンドライン管理ツールの [コマンド](#) を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow Netcheck.ExePath
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Netcheck.ExePath <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Netcheck.ExePath -r
```

2. 設定にDr.Web Network Checkerコンポーネントの設定が含まれていない場合、または正しいパスを入力した後もエラーが継続する場合は、drweb-netcheck パッケージをインストールまたは再インストールしてください。



Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については [Dr.Web for UNIX Internet Gatewaysをインストールする](#) および [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#) のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *CloudDは使用できません*

エラーコード: x124

内部指定: EC_NO_CLOUDD

説明: Dr.Web Cloudサービスへの要求に必要なDr.Web CloudDが見つかりません。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。

エラーの解決

1. `drweb-cloudd` 実行ファイルへのパスを確認してください。必要に応じてパスを変更します([設定ファイル](#)の[CloudD] [セクション](#)にある `ExePath` パラメータ)。

または、コマンドライン管理ツールの [コマンド](#) を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow CloudD.ExePath
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset CloudD.ExePath <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset CloudD.ExePath -r
```

2. 設定にDr.Web CloudDコンポーネントの設定が含まれていない場合、または正しいパスを入力した後もエラーが継続する場合は、`drweb-cloudd` パッケージをインストールまたは再インストールしてください。

Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については [Dr.Web for UNIX Internet Gatewaysをインストールする](#) および [Dr.Web for UNIX Internet Gatewaysをアンインストールする](#) のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ: *予期せぬエラーです*

エラーコード: x125

内部指定: EC_UNEXPECTED_ERROR

説明: いずれかのコンポーネントの動作に、予期せぬエラーが発生しました。

考えられる原因やエラーの状況を特定するには、Dr.Web for UNIX Internet Gatewaysのログを参照してください(デフォルトでは、OSによって /var/log/syslog ファイルまたは /var/log/messages ファイルにあります)。また、[コマンド](#) `drweb-ctl log` を使用することもできます。



エラーの解決

1. 以下のコマンドを入力し、Dr.Web for UNIX Internet Gatewaysを再起動します。

```
# service drweb-configd restart
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡のうえ、エラーコードをお伝えください。

コードのないエラー

症状：Dr.Web ClamD、SpIDer Gate、Dr.Web ICAPDなどのコンポーネントがメッセージをスキャンしない。Dr.Web for UNIX Internet GatewaysのログにメッセージToo many open filesが表示される。

説明：データスキャンの負荷が大きいため、Dr.Web Network Checkerが利用可能なファイル記述子の制限を超えました。

エラーの解決

1. ulimit -nコマンドを使用して、アプリケーションで使用可能なオープンファイルの記述子数の上限を引き上げます（Dr.Web for UNIX Internet Gatewaysの記述子数のデフォルト上限は16384です）。



場合によっては、システムサービスsystemdは、指定した上限の変更を無視できます。

この場合、ファイル/etc/systemd/system/drweb-configd.service.d/limits.confを編集し（存在しない場合は作成し）、変更後の制限値を次のように指定します。

```
[Service]
LimitNOFILE=16384
```

systemdの利用可能な上限のリストはドキュメントman systemd.execで確認できます。

2. 上限を変更したら、次のコマンドを実行してDr.Web for UNIX Internet Gatewaysを再起動します。

```
# service drweb-configd restart
```

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡ください。

症状：WebブラウザがDr.Web管理Webインターフェースへの接続を確立できない。Dr.Webアンチウイルスソリューションのコンポーネントが、実行中のプロセスのリスト(ps ax | grep drweb)に含まれていない。drweb-ctl rawscan以外のdrweb-ctl <command>を実行しようとする、次のいずれかのエラーが発生する。

```
Error: connect: No such file or directory: "<path>/ .com.drweb.public"
```

または

```
Error: connect: Connection refused: "<path>/ .com.drweb.public".
```

説明：設定デーモンDr.Web ConfigDが使用できないため、Dr.Web for UNIX Internet Gatewaysを起動できません。



エラーの解決

1. 次のコマンドを実行します。

```
# service drweb-configd restart
```

これによってDr.Web ConfigDとDr.Web for UNIX Internet Gatewaysが再起動します。

2. このコマンドがエラーメッセージを返した場合、または効果がない場合は、drweb-configdコンポーネント(パッケージ)を個別にインストールしてください。



これは、PAM認証がシステムで使用されていないことを意味する場合があります。その場合は、PAMをインストールして設定します(PAMがないとDr.Web for UNIX Internet Gatewaysは正しく動作できません)。

3. エラーが解決しない場合は、Dr.Web for UNIX Internet Gatewaysを削除してから再度インストールしてください。

Dr.Web for UNIX Internet Gatewaysまたはそのコンポーネントのインストールとアンインストールの方法については、[Dr.Web for UNIX Internet Gatewaysをインストールする](#)および[Dr.Web for UNIX Internet Gatewaysをアンインストールする](#)のセクションを参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡ください。

症状

1. SpIDer Gateを無効にした後、すべてのネットワーク接続が切断され(SSHおよびFTPプロトコル経由での送信と、場合によっては受信も)、再確立することができない。
2. NetFilter(iptables)ルールを検索するために

```
# iptables-save | grep "comment --comment --comment"
```

を使用すると、空以外の結果が返ってくる。

説明: このエラーは、1.4.15より以前のバージョンのNetFilter(iptables)の異常動作に関連しています。この内部エラーのため、SpIDer Gateが一意的ラベル(コメント)が付いたルールをルールリストに追加すると、そのルールは誤って追加されます。その結果、SpIDer Gateはシャットダウン時に接続のリダイレクトルールを削除できません。

エラーの解決

1. SpIDer Gateモニターを再度有効にしてください。
2. SpIDer Gateを無効にする必要がある場合は、以下のコマンドを使用してNetFilter(iptables)の不正なルールを削除してください。

```
# iptables-save | grep -v "comment --comment --comment" | iptables-restore
```



`iptables-save`および`iptables-restore`コマンドにはroot権限が必要です。権限を昇格するには`su`または`sudo`コマンドを使用できます。

このコマンドは、正しくないコメントを持つすべてのルール（例：同じトラフィックのリダイレクトを実行する、他のアプリケーションによって追加されたものなど）を削除します。

追加情報

- この問題の発生を防ぐため、お使いのOSをアップグレードすることを推奨します（または、少なくともNetFilterをバージョン1.4.15以降にすることを推奨します）。
- また、`iptables`ユーティリティを使用して必要なルールを指定することで、接続を手動でSpIDer Gateへリダイレクトさせる場合は、Dr.Web Firewallの設定でSpIDer Gateへの接続のリダイレクトを手動モードに切り替えることができます（この方法は推奨されません）。
- 詳細は、マニュアル`man: drweb-firewall(1)`、`drweb-gated(1)`、`iptables(8)`を参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡ください。



付録G. 略語のリスト

本マニュアルでは、次の略語を詳しく解説することなく使用しています。

表記規則	説明
<i>AD</i>	Microsoft Active Directory(マイクロソフトアクティブディレクトリ)
<i>DN</i>	(LDAP) Distinguished Name(識別名)
<i>FQDN</i>	Fully Qualified Domain Name(完全修飾ドメイン名)
<i>GID</i>	Group ID(システムユーザーグループID)
<i>GNU</i>	GNUプロジェクト(GNU is Not Unix)
<i>HTML</i>	HyperText Markup Language(ハイパーテキストマークアップ言語)
<i>HTTP</i>	HyperText Transfer Protocol(ハイパーテキスト転送プロトコル)
<i>HTTPS</i>	HyperText Transfer Protocol Secure(ハイパーテキスト転送プロトコルセキュア)(SSL/TLS経由)
<i>ICAP</i>	Internet Content Adaptation Protocol(インターネットコンテンツアダプテーションプロトコル)
<i>ID</i>	Identifier(識別子)
<i>IP</i>	Internet Protocol(インターネットプロトコル)
<i>LDAP</i>	Lightweight Directory Access Protocol(ライトウェイトディレクトリアクセスプロトコル)
<i>MBR</i>	Master Boot Record(マスターブートレコード)
<i>OID</i>	(SNMP) Object ID(オブジェクトID)
<i>OS</i>	Operating System(オペレーティングシステム)
<i>PID</i>	Process ID(システムプロセスID)
<i>PAM</i>	Pluggable Authentication Modules(プラグブル認証モジュール)
<i>RPM</i>	Red Hat Package Manager(Red Hatパッケージマネージャー)
<i>RRA</i>	Round-Robin Archive(ラウンドロビンアーカイブ)
<i>RRD</i>	Round-Robin Database(ラウンドロビンデータベース)
<i>SNI</i>	Server Name Indication(サーバー名表示)
<i>SNMP</i>	Simple Network Management Protocol(シンプルネットワークマネジメントプロトコル)



表記規則	説明
<i>SP</i>	Service Pack(サービスパック)
<i>SSH</i>	Secure Shell(セキュアシェル)
<i>SSL</i>	Secure Sockets Layer(セキュアソケットレイヤー)
<i>TCP</i>	Transmission Control Protocol(伝送制御プロトコル)
<i>TLS</i>	Transport Layer Security(トランスポート層セキュリティ)
<i>UID</i>	User ID(システムユーザーID)
<i>URI</i>	Uniform Resource Identifier(ユニフォームリソースアイデンティファイア)
<i>URL</i>	Uniform Resource Locator(ユニフォームリソースロケータ)
<i>VBR</i>	Volume Boot Record(ボリュームブートレコード)

